# Collabora and NextCloud SAML federation pilot

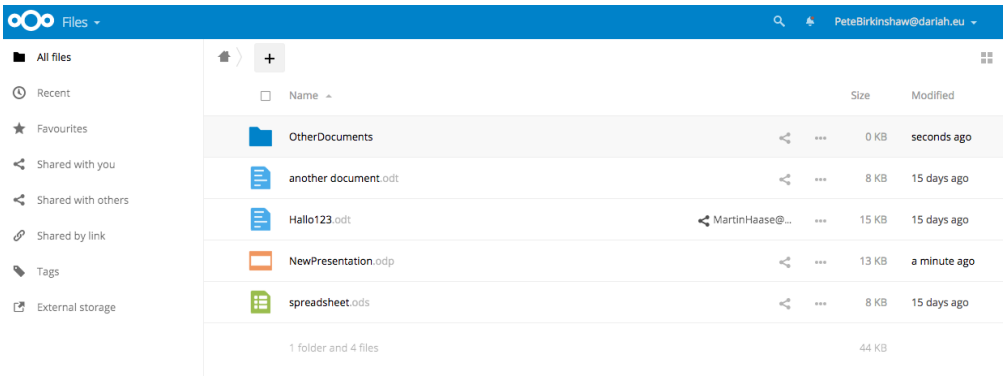
## Introduction

Documents are at the heart of most projects: people create and share text, spreadsheets, presentations and images. Federated access management has been widely used to control access to published documents, but its use in collaborative creation has usually been limited to wikis and content management systems. Office documents are usually created offline. This pilot explored the use of two new applications that can be used together to provide federated access to both file management and office document creation and collaborative editing.

## Components

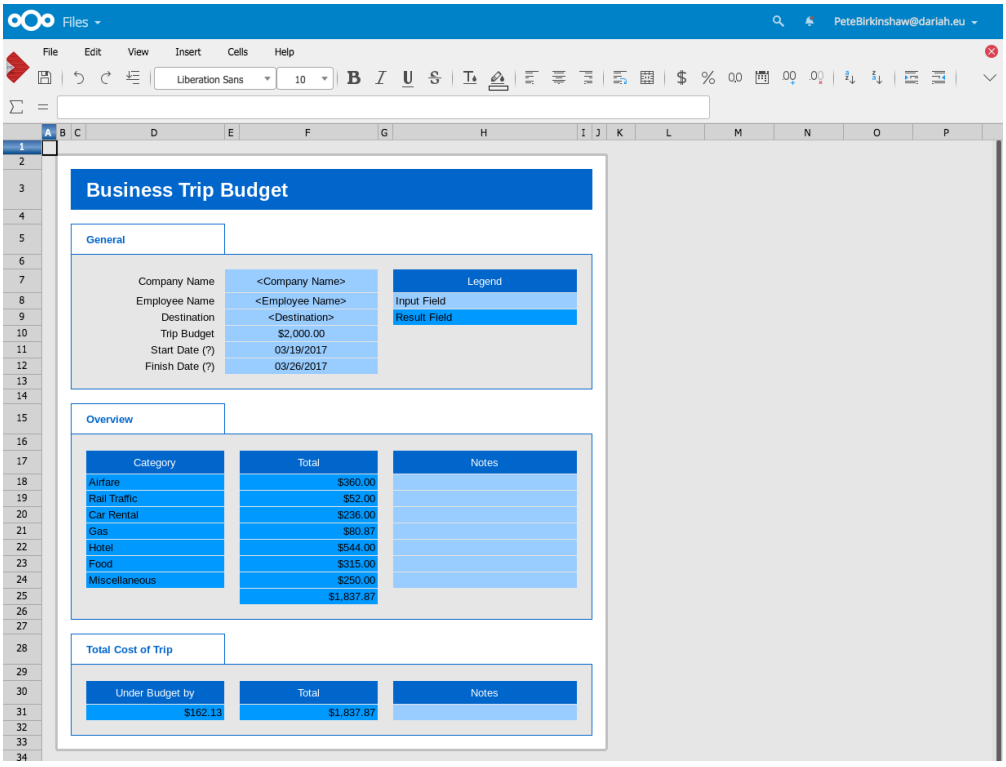
### NextCloud

NextCloud is a web-based document management service. Documents can be uploaded and downloaded via a web interface, or synchronised with local files. Files can be shared with other users. NextCloud was recently forked from OwnCloud. They remain very similar, but NextCloud offers new built-in federated access features using SAML in its free version. We used NextCloud's free edition in this pilot, but the commercially supported edition of OwnCloud may be used in a similar way.




### Collabora Online - LibreOffice for the web

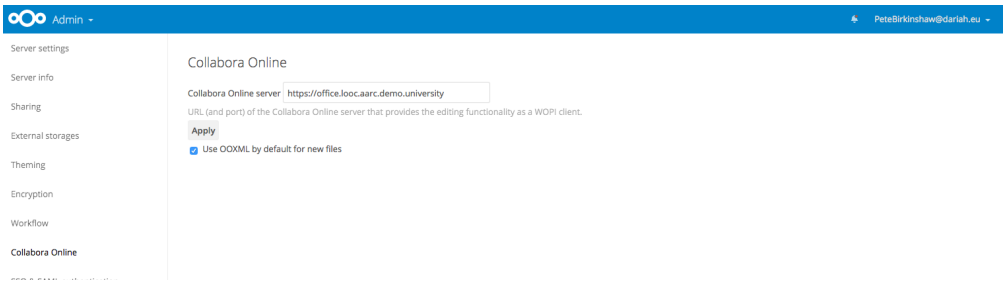
Collabora Online is new software that allows the LibreOffice/OpenOffice office suite to run as a shared web application. Most of the desktop LibreOffice's functionality is available to users in a web page, with the added feature of simultaneous collaborative editing - users can work on the same document at the same time.



# Integrating NextCloud and Collabora Online

Collabora Online provides a basic administration user interface, minimal configuration files, and a generic WOPI API (as used by Microsoft Office). It runs as a web application behind an Apache or NGINX reverse-proxy with SSL. Authentication and authorisation are handled via WOPI and resemble Oauth. As such it requires a second application to act as the primary user interface and authentication provider.

NextCloud is a PHP application and performs the role of , user interface, document store and WOPI authentication server. Collabora Online compatibility is now available via a bundled plugin and the only configuration needed is the URL for the Collabora service. When users open a file in NextCloud control is passed to Collabora Online, and the office application interface appears.



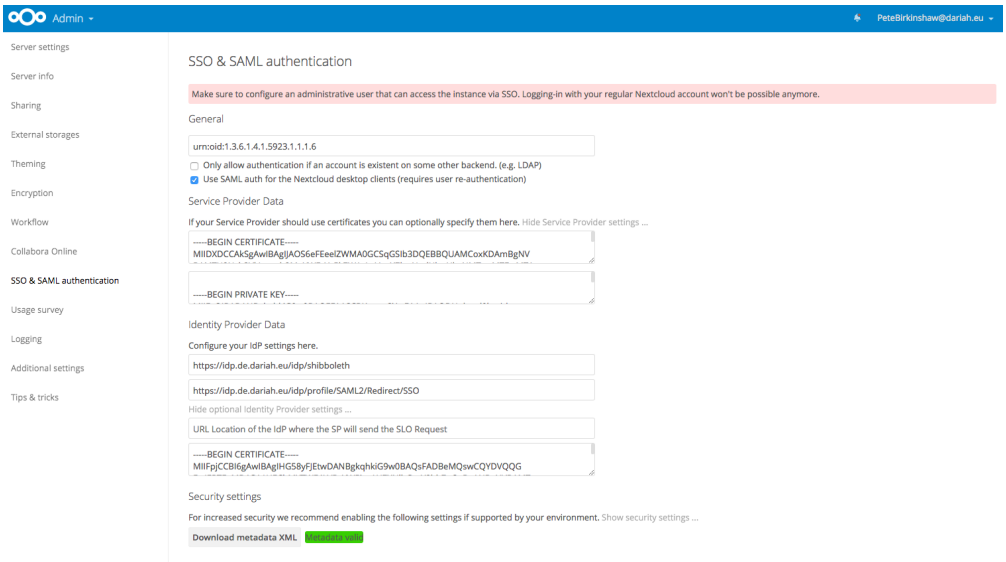

A single Collabora Online service can be used by more than one NextCloud front-end.

# AAI Integration Options

NextCloud needs a means of handling its own authentication. Two options are currently available for federated authentication: a built-in SAML SP, and a external SSO option that relies on the web server handling authentication.

## Built-In SAML

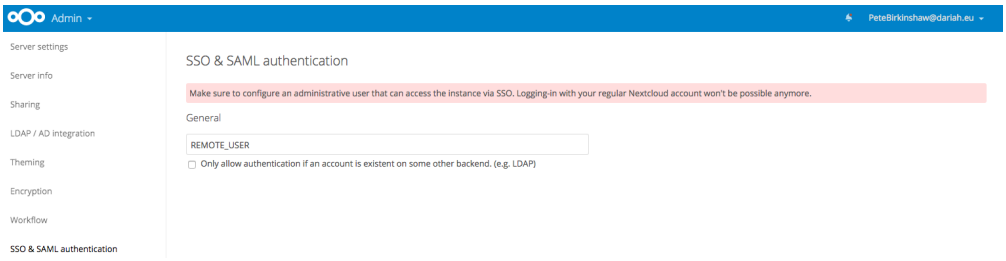
NextCloud's SAML implementation is currently rather limited, and only supports one IdP. This means that a proxy IdP would be needed to provide fully federated access to users.




More advanced SAML features are planned and development seems to be active.

## External authentication

The second SSO option is to rely on the web server (such as Apache or NGINX) and use basic user information passed as environment variables such as REMOTE_USER.

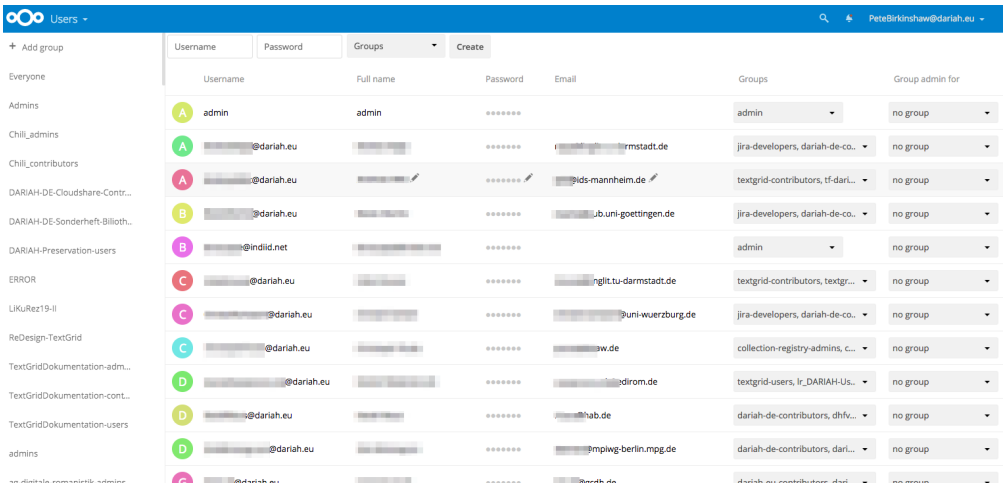



This means that the Shibboleth SP software, OpenID Connect or even Kerberos can be used, but integration is weak - only the username is available.

## Aggregating attributes from LDAP

It is possible to combine federated authentication with LDAP for additional attributes, and to require presence in the LDAP directory for authentication to succeed.

This would hinder usage across a federation (since users would not exist in the LDAP directory) but may help research organisations, as group membership and access control can be handled by a community LDAP server.



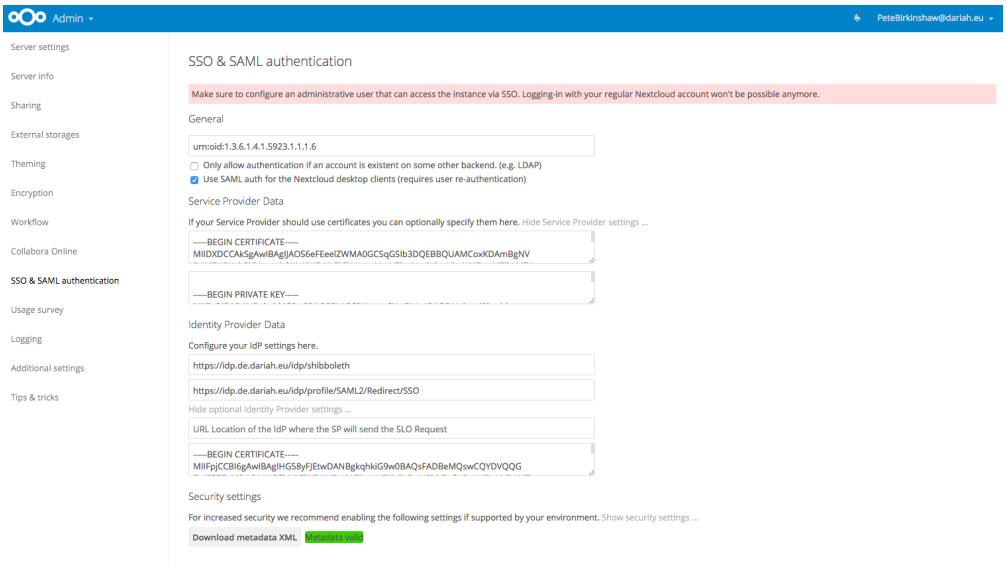

# Pilot Implementations

Three different demonstrations were set up, so that different features and integration combinations could be explored.

## Demonstration 1: Integrated SAML with one IdP

Built-in SAML

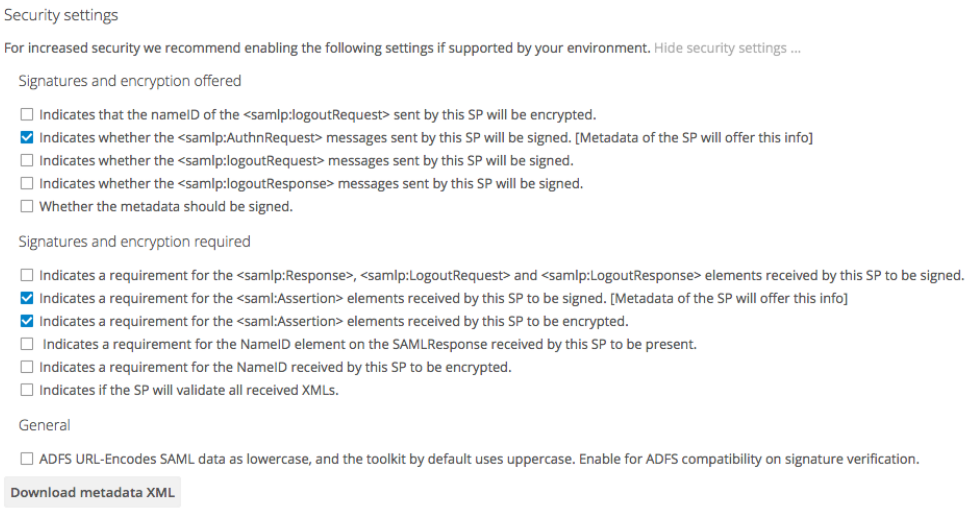
https://cloud.looc.aarc.demo.university/nextcloud/index.php/




Configured using NextCloud's built-in SAML to connect to one IdP as if used by a single university or research community using a proxy IdP.

Keys were created using the Shibboleth SP keygen tool and pasted into the configuration form in NextCloud. EPPN was used for NextCloud usernames (identified by URN)

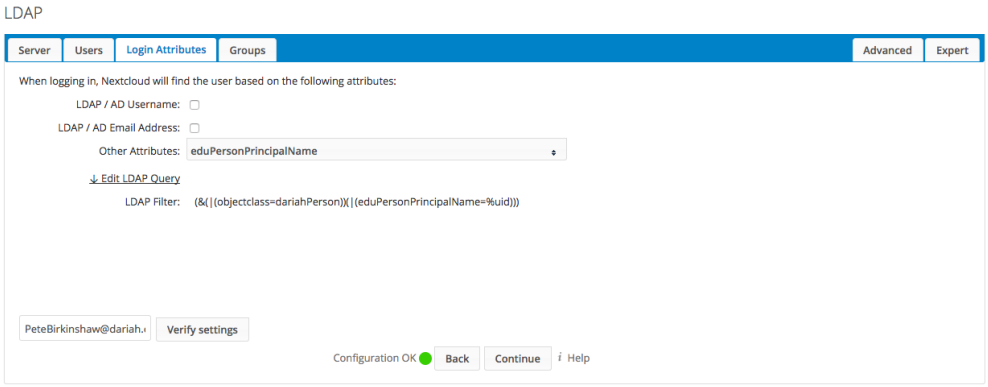
NextCloud generated its own metadata, but the expiry date was only for a few days and so was removed before sharing. Various combinations of encryption and signing can be set.




## Demonstration 2: External authentication (SAML) plus LDAP

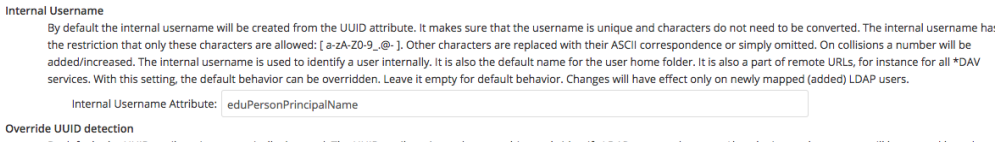
External SSO

https://cloud.aarc.federated-example.website/nextcloud/index.php/apps/files/




Configured to use a single IDP, using the external SSO plugin and a conventional Shibboleth SP. NextCloud was configured to search an LDAP directory for records matching the SAML-authenticated user's EduPersonPrincipalName. LDAP was also used to discover which groups a user was a member of. These groups can be used for access control.

Session lifespans for the external authentication service (Shibboleth SP) and Nextcloud's own sessions can become out-of-sync, and require some adjustments to work together consistently.




### Demonstration 3: Integrated SAML with a federated IdP Proxy

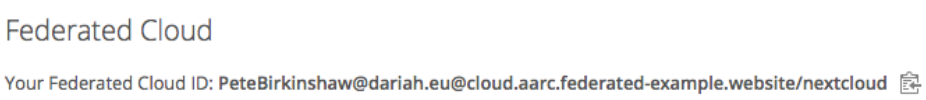
Built-in SAML

https://files.looc.aarc.federated-example.website

(Work-in-progress) A similar pilot to the Demonstration 1 but configured to use the Terena Proxy so that it's easier for a wider range of people to log in.

## An Aside: Federated data storage

NextCloud supports "federated sharing", which permits users to share files between different NextCloud services, and browse user directories on other services. Users are given a globally unique scoped identifier that resembles EduPersonPrincipalName. If EPPN is used as the NextCloud username then a user's identifier is scoped twice.




The External Storage plugin allows remote data storage to be used, including other NextCloud or OwnCloud services, Windows shares and NFS.

## Caveats

## Speed

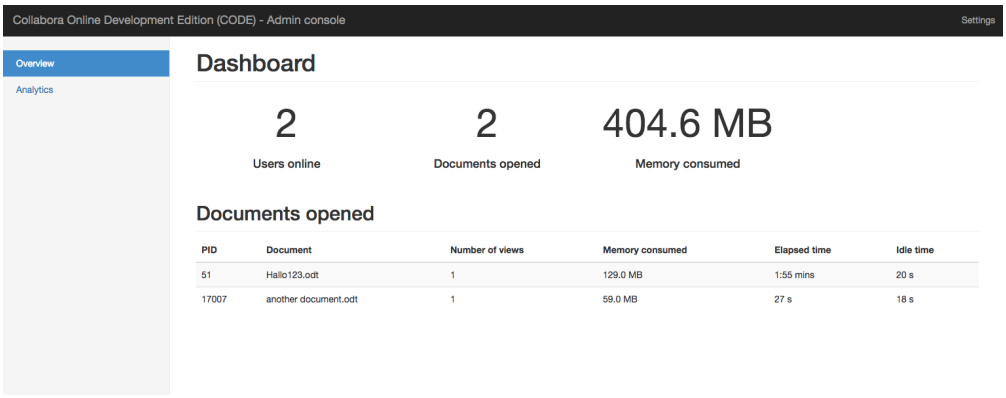
The display of Collabora is generated by sending many tile-like images over the web as individual files, and is rather slow. Over a normal broadband internet connection the display is not quite fast enough to keep up with typing.

Over a much faster connection such as a LAN the speed is greatly improved.

### The Open Source Collabora Online package has restrictions

The CODE (Collabora Online Developer Edition) Docker container used in these pilots is limited to 10 concurrent users. Collabora offer a commercial edition with no limits.

However, there is an unofficial project to help with installing an alternative open source version of the Collabora Online software without these limitations, and without Docker.




### Admin accounts must be created before switching to SSO

Admin users (who are able to configure the service) must be created in Nextcloud, using EPPNs, in advance, before SSO is enabled.

### Cannot easily change SSO methods

NextCloud's SSO plugin offers a choice between the built-in SAML and using external authentication, and it does not seem to be possible to easily switch from one to the other.

### Application passwords are still required

Users will need to create their own passwords in NextCloud to use for syncing files and other non-web access.

## Further Information

- NextCloud admin manual
- Nextcloud SAML documentation
- CODE edition of Collabora
- LibreOffice Online installer project (a community alternative to CODE)
- NextCloud app passwords, for non-web devices