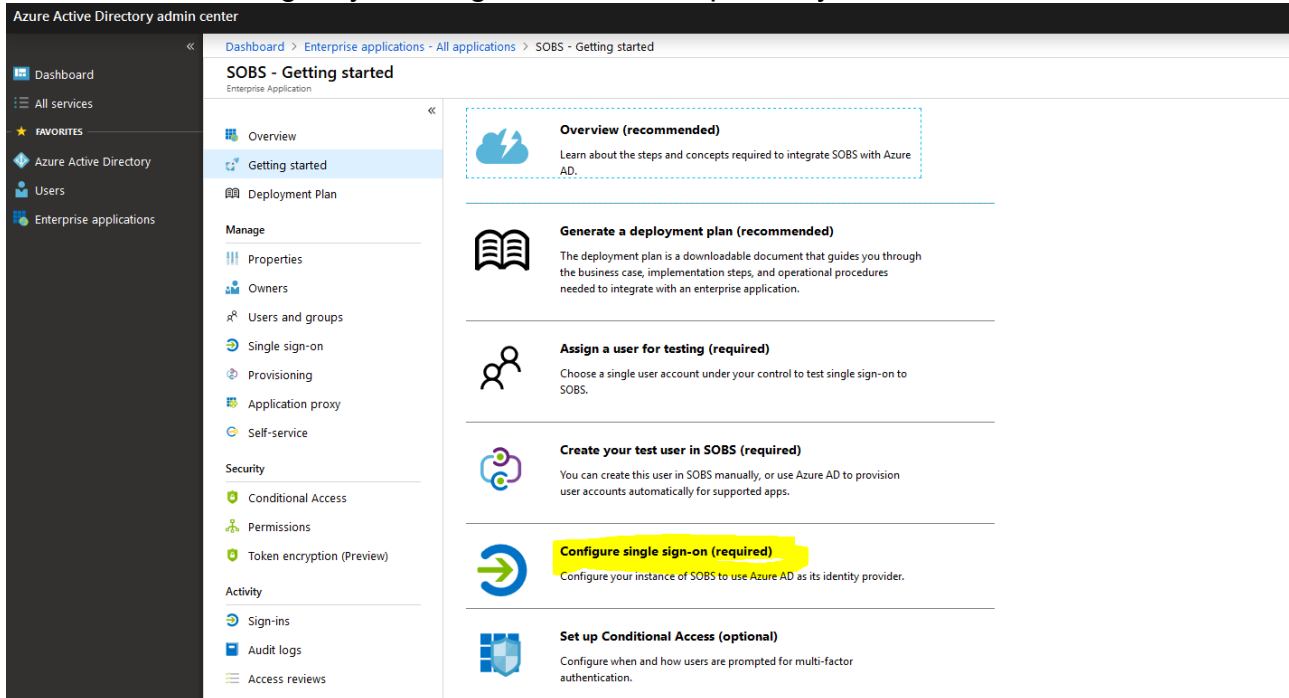


SAML

SOBS and Office365

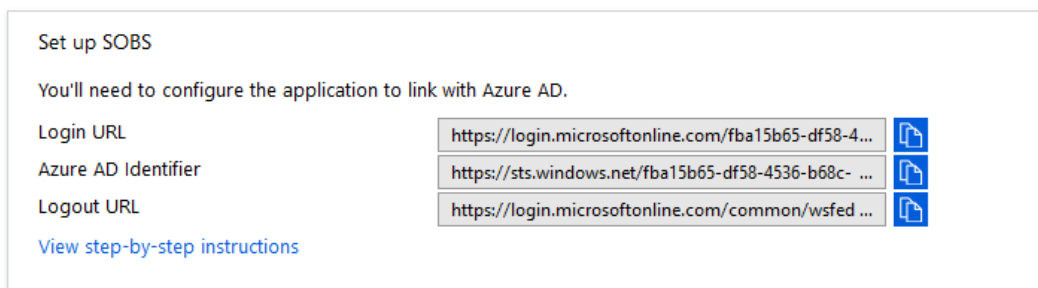
Special thanks to Shane Clay for his assistance with this documentation.

From Office 365 begin by creating a new service, probably called “SOBS”:



The screenshot shows the Azure Active Directory admin center interface. The left-hand navigation pane includes sections for Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area is titled "SOBS - Getting started" and lists several tasks: Overview (recommended), Generate a deployment plan (recommended), Assign a user for testing (required), Create your test user in SOBS (required), Configure single sign-on (required), and Set up Conditional Access (optional). The "Configure single sign-on (required)" task is highlighted with a yellow background.

You will need some settings from Office 365 first – these will be added into the SOBS saml configuration:



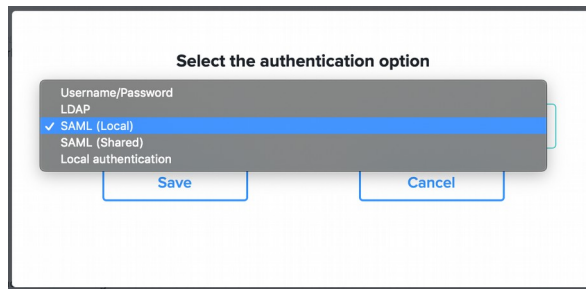
The screenshot shows a configuration page titled "Set up SOBS". It instructs the user to configure the application to link with Azure AD. The following settings are listed:

Login URL	https://login.microsoftonline.com/fba15b65-df58-4...
Azure AD Identifier	https://sts.windows.net/fba15b65-df58-4536-b68c- ...
Logout URL	https://login.microsoftonline.com/common/wsfed ...

[View step-by-step instructions](#)

Login into SOBS normally.

1. Click on the school name (bottom left) to reveal another menu
2. Click on the “School configuration” menu entry
3. From the top menu click on “Authentication”
4. Select the “SAML (Local)” option and then click “Save”



Authentication

Select

Edit

Selected authentication method

SAML (Local)

SAML Login URL:

<https://sobs.com.au/ui/login.php?schoolid=15>

SAML Entries: [Add](#)

Now you can use the “Add” link to add SAML entries from the Azure information in the image on the previous page.

1. The first entry is the BaseDomain, this is the Azure AD Identifier
2. Next you will add the SingleSignInService, this is the “Login URL”
3. Next you will add the SingleLogoutService, this is the “Logout URL”
4. The last entry is the NameIDFormat (this has a default value for SAML2, however you can change it if necessary)
5. You will also need to upload a token signing certificate (from Azure). Use the “Base64” certificate (See the image below)

Now use the “Generate metadata” button to download the metadata in an XML format.

Upload this metadata file to your Office 365 Azure configuration using the “Upload metadata file” as in the image below.

Dashboard > Enterprise applications - All applications > SOBS - Single sign-on > SAML-based sign-on

SOBS - SAML-based sign-on

Enterprise Application

[Upload metadata file](#)
[Change single sign-on mode](#)
[Switch to the old experience](#)
[Test this application](#)

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating SOBS.

- #### Basic SAML Configuration

Identifier (Entity ID)	https://sobs.com.au/simplesaml/module.php/saml/sp/metadata.php/sobs-sp
Reply URL (Assertion Consumer Service URL)	https://sobs.com.au/simplesaml/module.php/saml/sp/saml2-acs.php/sobs-sp
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- #### User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Role	"staff"
User-Name	user.onpremisesamaccountname
Unique User Identifier	user.userprincipalname
- #### SAML Signing Certificate

Status	Active
Thumbprint	588704627EA2D6DCE82879A01F29AE9177809AEA
Expiration	4/24/2022, 11:52:41 AM
Notification Email	shane.clay@stcolumba.sa.edu.au
App Federation Metadata Url	https://login.microsoftonline.com/fba15b65-df58-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

You will need to create to additional attributes / claims, as in the above image. One is called "Role" - this tells SOBS that the user logging in is a staff member and will assign staff security to the SOBS account (as it may be automatically created). The second is the "User-Name" which will be the SOBS login username (and probably the Azure network username).

Lastly, you will need to allow each user to use this SAML authentication option. This can allow you to restrict students from accessing SOBS if that is required.

Dashboard > Enterprise applications - All applications > SOBS - Users and groups

SOBS - Users and groups

Enterprise Application

[Add user](#)
[Edit](#)
[Remove](#)
[Update Credentials](#)
[Columns](#)

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
Shane Clay	User	User
St Columba Staff	Group	User

NOTE: As of April 2023 the Azure test function does not work with SOBS, however the normal SAML login process works fine.