



Azure Single Sign-On (SSO) Integration with Campus Cafe Documentation

Contents

Introduction.....	2
Prerequisites.....	2
(OPTION 1) Single Sign-On Integration via Azure Gallery	3
Configure and test Azure AD single sign-on for Campus Café.....	3
Configure Azure AD SSO	3
(OPTION 2) Single Sign-On Integration via Custom SAML Integration.....	6
Create an Azure AD test user.....	10
Assign the Azure AD test user.....	10
Configure Campus Cafe SSO	11
Test SSO	11
Additional Resources	11

Introduction

The following guide will help you establish a SAML connection between your Azure Active Directory (Azure AD) and Campus Café. When you integrate Campus Café with Azure AD, you can:

- Control in Azure AD who has access to Campus Café.
- Enable your users to be automatically signed-in to Campus Café with their Azure AD accounts.
- Manage your accounts in one central location - the Azure portal.

There are two options for adding an integration with Campus Café: via the Azure Gallery (preferred), or via custom SAML integration.

Prerequisites

To get started, you will need the following items:

- An Azure AD subscription. If you don't have a subscription, you can get a [free account](#).
- Campus Café single sign-on (SSO) enabled subscription.
 - Campus Café will provide you with a three-letter identifier for your cloud-based Campus Café deployment.

(OPTION 1) Single Sign-On Integration via Azure Gallery

In this tutorial, you configure and test Azure AD SSO in a test environment.

- Campus Café supports **SP** initiated SSO
- Once you configure Campus Café you can enforce session control, which protect exfiltration and infiltration of your organization's sensitive data in real-time. Session control extend from Conditional Access. [Learn how to enforce session control with Microsoft Cloud App Security](#).

To configure the integration of Campus Café into Azure AD, you need to add Campus Café from the gallery to your list of managed SaaS apps.

1. Sign in to the [Azure portal](#) using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add new application, select **New application**.
5. In the **Add from the gallery** section, type **Campus Café** in the search box.
6. Select **Campus Café** from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Configure and test Azure AD single sign-on for Campus Café

Configure and test Azure AD SSO with Campus Café using a test user called **B.Simon**. For SSO to work, you need to establish a link relationship between an Azure AD user and the related user in Campus Café.

To configure and test Azure AD SSO with Campus Café, complete the following building blocks:

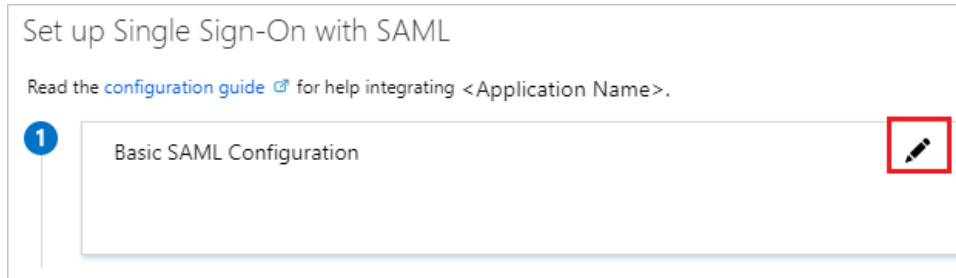
1. [Configure Azure AD SSO](#) - to enable your users to use this feature.
 - [Create an Azure AD test user](#) - to test Azure AD single sign-on with B.Simon.
 - [Assign the Azure AD test user](#) - to enable B.Simon to use Azure AD single sign-on.
2. [Configure Campus Café SSO](#) - to configure the single sign-on settings on application side.
 - [Create Campus Café test user](#) - to have a counterpart of B.Simon in Campus Café that is linked to the Azure AD representation of user.
3. [Test SSO](#) - to verify whether the configuration works.

Configure Azure AD SSO

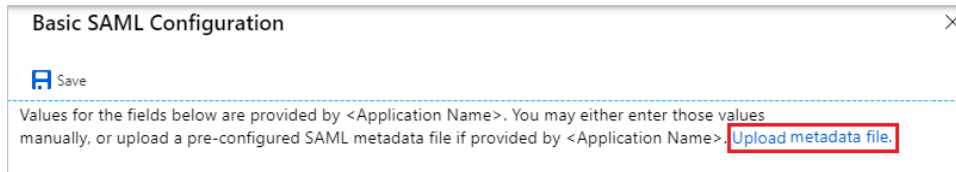
Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the [Azure portal](#), on the **Campus Café** application integration page, find the **Manage** section and select **single sign-on**.

2. On the **Select a single sign-on method** page, select **SAML**.
3. On the **Set up single sign-on with SAML** page, click the edit/pen icon for **Basic SAML Configuration** to edit the settings.



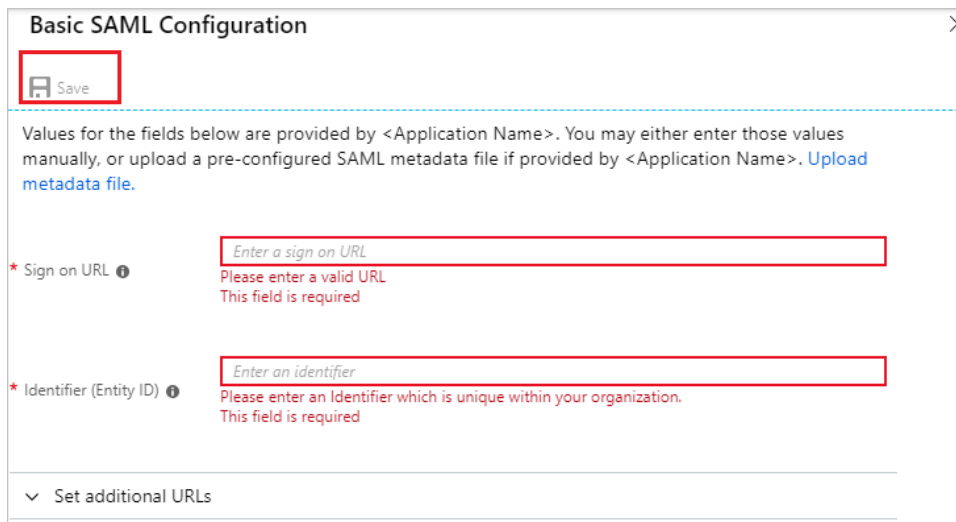
1. On the **Basic SAML Configuration** section, if you have **Service Provider metadata file** from Campus Café, perform the following steps:
 - a. Click **Upload metadata file**.



- b. Click on **folder logo** to select the metadata file and click **Upload**.



- c. After the metadata file is successfully uploaded, the **Identifier** value gets auto populated in the Basic SAML Configuration section.

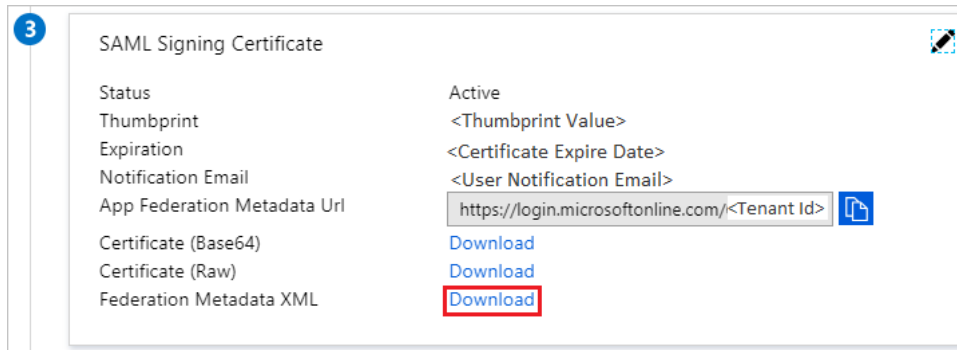


In the **Sign-on URL** text box, type a URL using the following pattern:

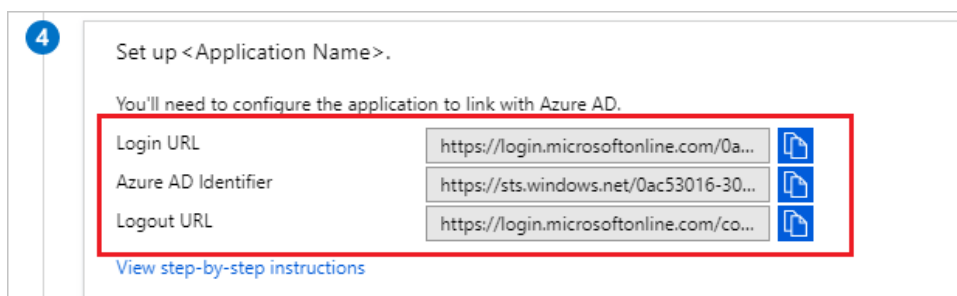
`https://{SSO}-web.scansoftware.com/cafeweb/loginso`

Please Note: The **Identifier** value – {SSO} in the examples within this document – should get auto populated from the metadata supplied to you from Campus Café. Please fill in the value manually according to the three-letter tenant identifier that was provided to you by Campus Café if it does not. The Sign-on URL value used in this document is **not real** and will **not work**. If you do not have an identifier please contact the [Campus Café Client support team](#) to get this value and/or the value to use as the sign-on URL.

2. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Federation Metadata XML** and select **Download** to download the certificate and save it on your computer.



3. On the **Set up Campus Café** section, copy the appropriate URL(s) and provide this information to the [Campus Café Client support team](#).

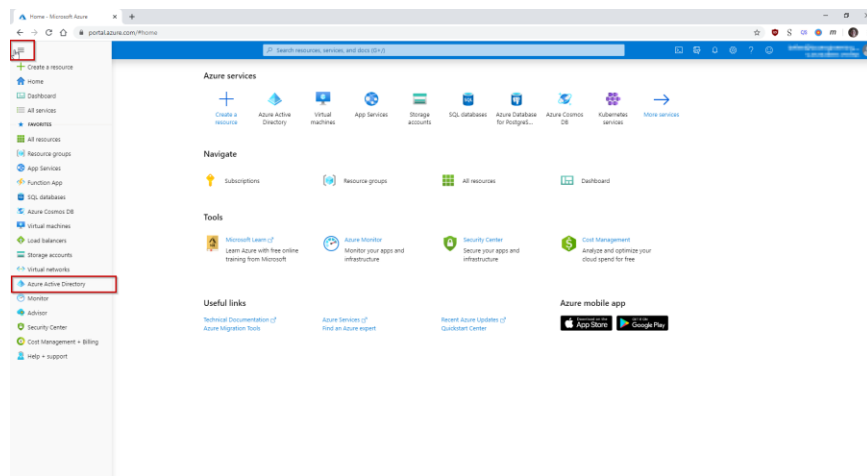


Campus Café will use this information to configure your tenant to correctly connect to Azure AD.

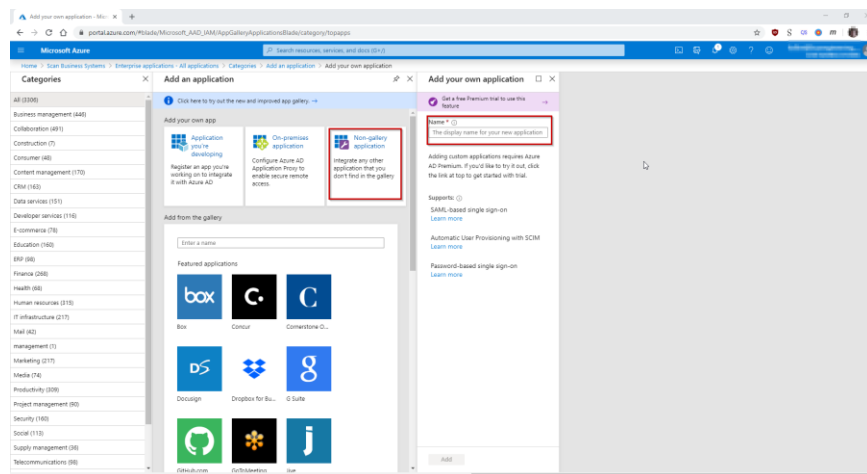
(OPTION 2) Single Sign-On Integration via Custom SAML Integration

The following instructions document how to on-board your Campus Café Single Sign-On (SSO) to Azure Active Directory if you currently have access to an Azure AD P1 or P2 license and prefer not to integration via the gallery.

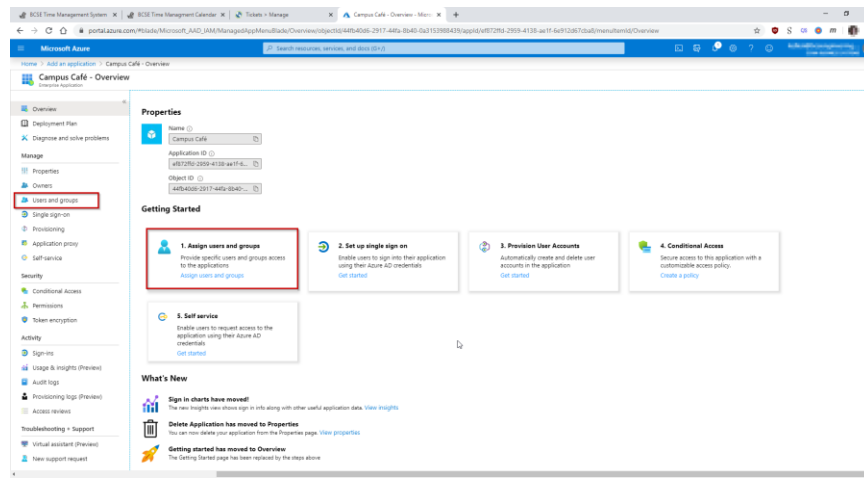
1. From the Azure portal (<https://portal.azure.com/>) select Azure Active Directory, from the upper left “hamburger” menu:



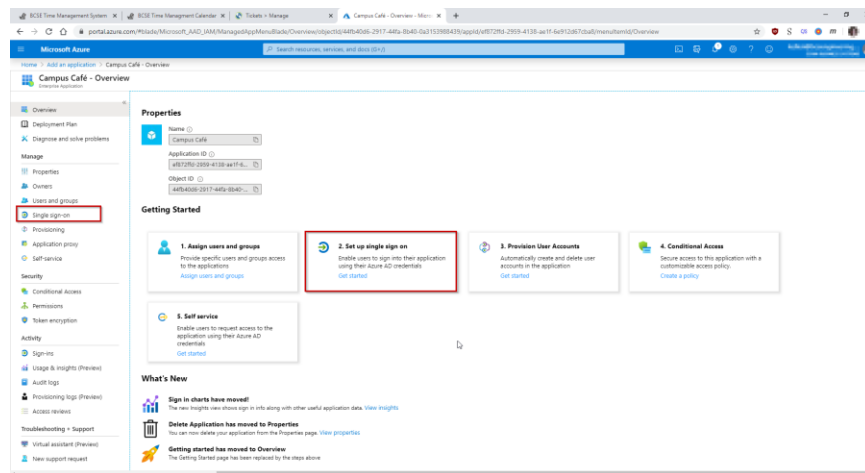
2. Then, select “Enterprise Applications”, followed by “New Application”.
3. Select “Non-gallery application”
4. Provide a Name for the Application, we suggest “Campus Café”



5. Select “Add”
6. You will be presented with the following page after successfully adding the page.



7. Select “Users and Groups” from the left-side menu, or, “Getting Started Step #1 Assign users and groups.”
8. Here you may select individual users who have access to the application, or assign groups with access, as you desire. We strong recommend using Group-based allowance for the application, and the most-typical selection would be allowance for Students, Faculty, and Administrators (though this may vary depending upon your current needs and where you are in the Campus Café on-boarding process).
9. Next, we will provision access via SSO. Select the “Single sign-on” tab in the left menu, or if you are back at the main application screen, you may select “Getting Started Step #2 Set up single sign-on.”




10. Under “Select a single sign-on method” select SAML.
11. This will immediately redirect you to the “SAML-based Sign-on” Configuration screen. This five-step process enables SAML SSO for your Campus Café instance. First, let us configure the “Basic SAML Configuration” by selecting the pencil icon in this box:

Basic SAML Configuration	
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

Note: you will need to know your 3-letter “tenant ID”, as all URLs used in the SAML process involve this code, and will take the form <https://{SSO}-web.scansoftware.com> where “{SSO}” is replaced by your tenant id. Throughout the rest of this documentation, we will use the tenant id “SSO” for demonstration purposes, however you will need to use the code provided for your organization throughout. If you do not have an identifier please contact the [Campus Café Client support team](#) to get this value.

12. Provide the EntityID, Reply URL, Sign on URL, Relay State, and Logout URL for your organization. The following template URLs are provided replace “SSO” with your 3-letter tenant id.

Basic SAML Configuration

 Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

✓

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

✓

Sign on URL ⓘ

✓

Relay State ⓘ

Logout Url ⓘ

✓

EntityID: <https://SSO-web.scansoftware.com/shibboleth>

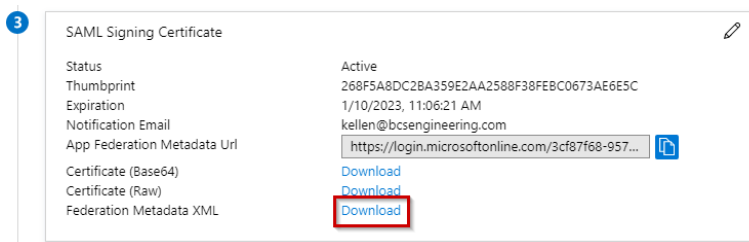
Reply URL: <https://SSO-web.scansoftware.com/Shibboleth.sso/SAML2/POST>

Sign on URL: <https://SSO-web.scansoftware.com/cafeweb/loginsso>

Relay State: <https://SSO-web.scansoftware.com/cafeweb/loginsso>

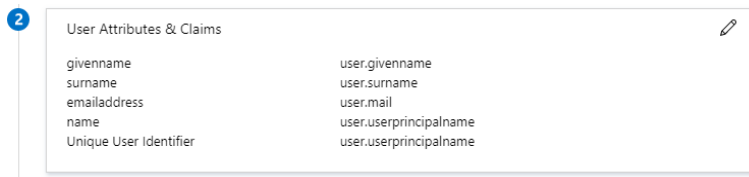
Logout URL: <https://SSO-web.scansoftware.com/Shibboleth.sso/Logout>

13. Next, please download the “Federation Metadata XML”. You will need to provide this to Campus Café in order to configure the integration on our end.



14. You should then click “Test” -> Sign in as Current User in order to test the integration.

Depending upon how your Campus Café users were imported into the Campus Café’s application database, some minor adjustments may be required within “Section 2: User Attributes and Claims”, however, by default and in most circumstances, the default Azure policies of releasing the following attributes will generally work:



with user.userprincipalname representing the Campus Café username. If you have created a custom integration attribute for Campus Café, be sure to contact your Campus Café integration specialist to assist in configuring the custom attribute.

Create an Azure AD test user

In this section, you will create a test user in the Azure portal called B.Simon.

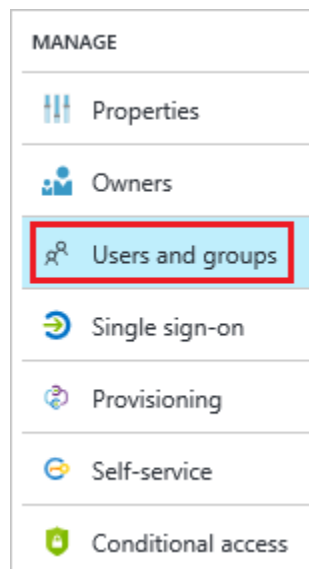
From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.

1. Select **New user** at the top of the screen.
2. In the **User** properties, follow these steps:
 - a. In the **Name** field, enter B.Simon.
 - b. In the **User name** field, enter the [username@domain.extension](#). For example, B.Simon@contoso.com.
 - c. Select the **Show password** check box, and then write down the value that is displayed in the **Password** box.
3. Click **Create**.

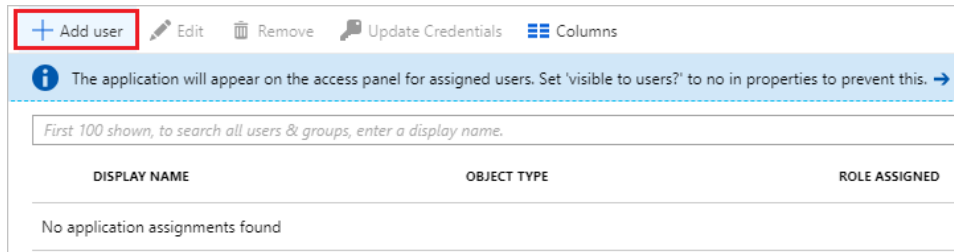
Assign the Azure AD test user

In this section, you will enable B.Simon to use Azure single sign-on by granting access to Campus Café.

1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select **Campus Café**.
3. In the app's overview page, find the **Manage** section and select **Users and groups**.



4. Select Add user, then select Users and groups in the Add Assignment dialog.



5. In the **Users and groups** dialog, select **B.Simon** from the Users list, then click the **Select** button at the bottom of the screen.
6. If you are expecting any role value in the SAML assertion, in the **Select Role** dialog, select the appropriate role for the user from the list and then click the **Select** button at the bottom of the screen.
7. In the **Add Assignment** dialog, click the **Assign** button.

Configure Campus Cafe SSO

To configure single sign-on on **Campus Café** side, you need to send the downloaded **Federation Metadata XML** and appropriate copied URLs from Azure portal to the [Campus Café support team](#). They set this setting to have the SAML SSO connection set properly on both sides.

Please also provide the name, email address, and password for the test user to the [Campus Café support team](#) so that they can create the test user in your tenant.

Test SSO

Sign out of your current Azure AD account in your web browser, and visit:

`https://{SSO}-web.scansoftware.com/cafeweb/loginsso`

You will need to replace {SSO} with your Campus Café tenant ID. When prompted enter your test user's username and password.

(Alternatively, you can also log the user in at office.com, and click the Campus Café tile in the Access Panel.)

In either case you should be automatically signed into the Campus Café for which you set up SSO. For more information about the Access Panel, see [Introduction to the Access Panel](#).

Additional Resources

Below you will find some handy links from Microsoft related to Azure Active Directory:

- [List of Tutorials on How to Integrate SaaS Apps with Azure Active Directory](#)
- [What is application access and single sign-on with Azure Active Directory?](#)

- [What is conditional access in Azure Active Directory?](#)
- [Try Campus Café with Azure AD](#)