

[Azure](#) / [Active Directory](#) / [Application management](#) / [SaaS application tu](#)

# Tutorial: Azure AD SSO integration with Azure AD SAML Toolkit

Article • 03/24/2022 • 6 minutes to read • [11 contributors](#)



## In this article

[Prerequisites](#)[Scenario description](#)[Add Azure AD SAML Toolkit from the gallery](#)[Configure and test Azure AD SSO for Azure AD SAML Toolkit](#)[Configure Azure AD SSO](#)[Configure Azure AD SAML Toolkit SSO](#)[Test SSO](#)[Next steps](#)

In this tutorial, you'll learn how to integrate Azure AD SAML Toolkit with Azure Active Directory (Azure AD). When you integrate Azure AD SAML Toolkit with Azure AD, you can:

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

## Prerequisites

To get started, you need the following items:

- An Azure AD subscription. If you don't have a subscription, you can get a [free account](#).
- Azure AD SAML Toolkit single sign-on (SSO) enabled subscription.
- Along with Cloud Application Administrator, Application Administrator can also add or manage applications in Azure AD. For more information, see [Azure built-in roles](#).

# Scenario description

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

- Azure AD SAML Toolkit supports **SP** initiated SSO.

## ⓘ Note

Identifier of this application is a fixed string value so only one instance can be configured in one tenant.

## Add Azure AD SAML Toolkit from the gallery

To configure the integration of Azure AD SAML Toolkit into Azure AD, you need to add Azure AD SAML Toolkit 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 **Azure AD SAML Toolkit** in the search box.
6. Select **Azure AD SAML Toolkit** 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 SSO for Azure AD SAML Toolkit

Configure and test Azure AD SSO with Azure AD SAML Toolkit 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 Azure AD SAML Toolkit.

To configure and test Azure AD SSO with Azure AD SAML Toolkit, perform the following steps:

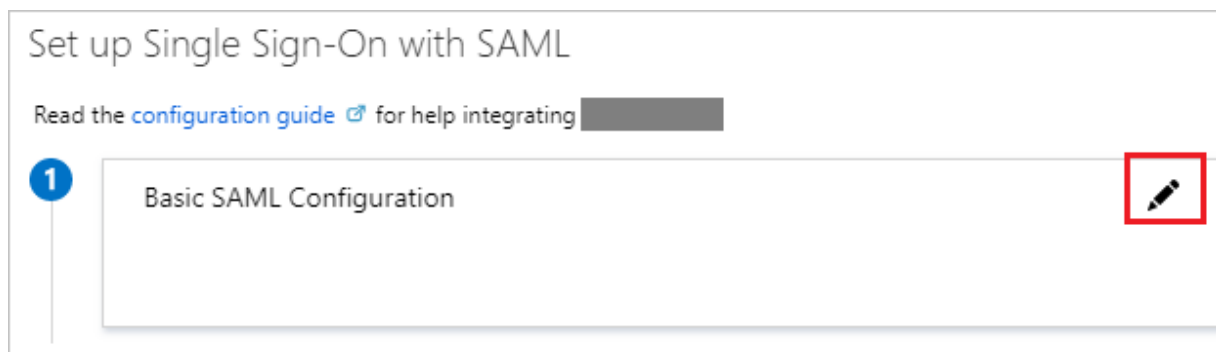
1. [Configure Azure AD SSO](#) - to enable your users to use this feature.
  - [Create an Azure AD test user](#) - to test Azure AD single sign-on with B.Simon.

- **Assign the Azure AD test user** - to enable B.Simon to use Azure AD single sign-on.
2. **Configure Azure AD SAML Toolkit SSO** - to configure the single sign-on settings on application side.
    - **Create Azure AD SAML Toolkit test user** - to have a counterpart of B.Simon in Azure AD SAML Toolkit that is linked to the Azure AD representation of user.
  3. **Test SSO** - to verify whether the configuration works.

## Configure Azure AD SSO

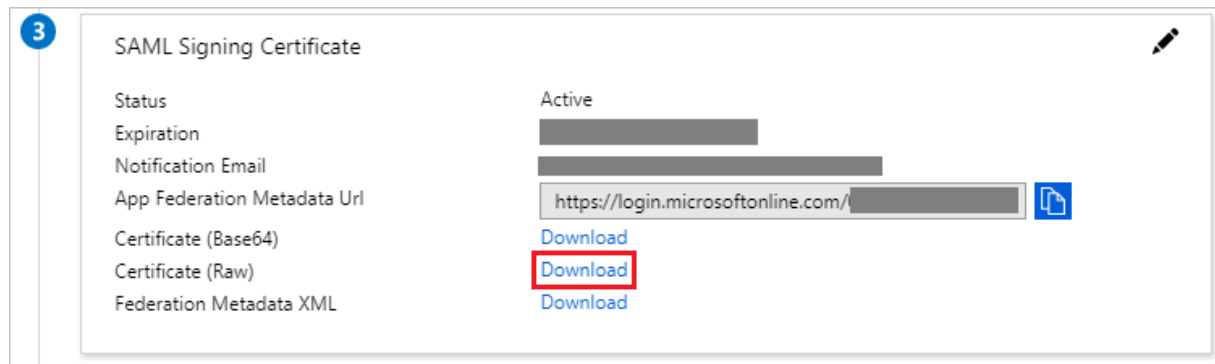
Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **Azure AD SAML Toolkit** 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 pencil icon for **Basic SAML Configuration** to edit the settings.

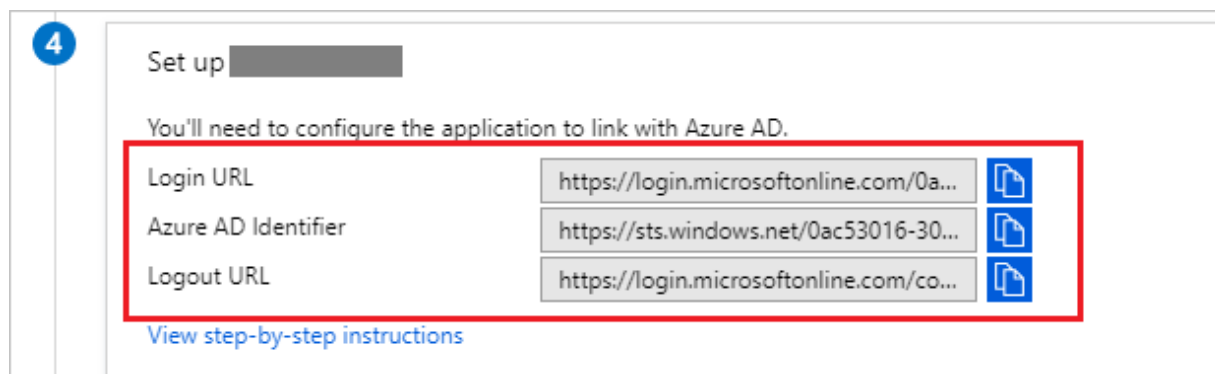


4. On the **Basic SAML Configuration** section, perform the following steps:
  - a. In the **Reply URL** text box, type the URL:  
`https://samltoolkit.azurewebsites.net/SAML/Consume`
  - b. In the **Sign on URL** text box, type the URL:  
`https://samltoolkit.azurewebsites.net/`
5. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Certificate (Raw)** and select **Download** to download the certificate and

save it on your computer.



6. On the **Set up Azure AD SAML Toolkit** section, copy the appropriate URL(s) based on your requirement.



## Create an Azure AD test user

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

1. From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.
2. Select **New user** at the top of the screen.
3. In the **User** properties, follow these steps:
  - a. In the **Name** field, enter B.Simon.
  - b. In the **User name** field, enter the username@companydomain.extension. For example, B.Simon@contoso.com.
  - c. Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
  - d. Click **Create**.

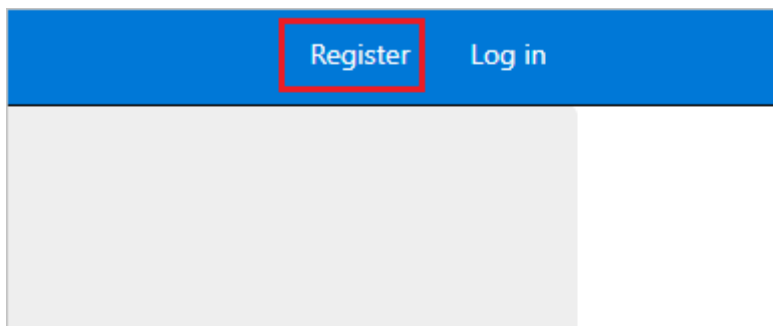
## Assign the Azure AD test user

In this section, you'll enable B.Simon to use Azure single sign-on by granting access to Azure AD SAML Toolkit.

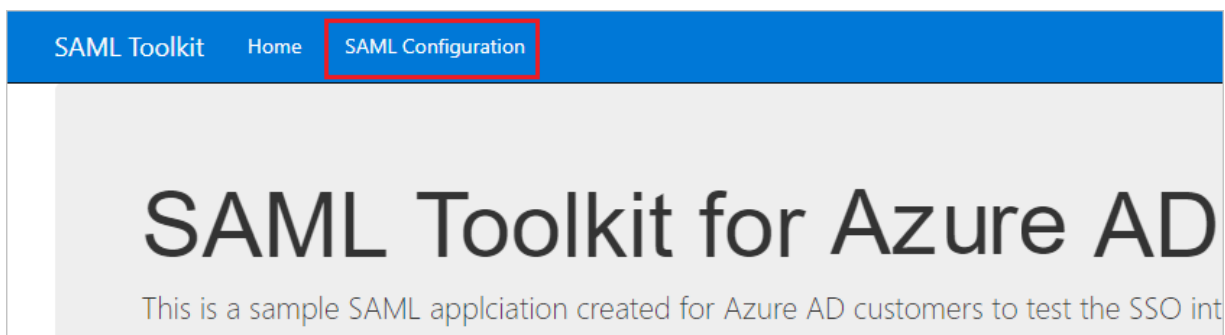
1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select **Azure AD SAML Toolkit**.
3. In the app's overview page, find the **Manage** section and select **Users and groups**.
4. Select **Add user**, then select **Users and 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 a role to be assigned to the users, you can select it from the **Select a role** dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the **Add Assignment** dialog, click the **Assign** button.

## Configure Azure AD SAML Toolkit SSO

1. Open a new web browser window, if you have not registered in the Azure AD SAML Toolkit website, first register by clicking on the **Register**. If you have registered already, sign into your Azure AD SAML Toolkit company site using the registered sign-in credentials.



2. Click on the **SAML Configuration**.



3. Click **Create**.

[SAML Toolkit](#) [Home](#) [SAML Configuration](#)

## SAML 2.0 Single sign-on Configuration

Create the configuration for your SAML 2.0 identity provider below. SAML Toolkit requires SAML assertions to include a NameID in connection below then it will provide you the SP initiated Login URL.

- Entity ID: **https://samltoolkit.azurewebsites.net**
- Assertion Consumer Service URL: **Copy Assertion Consumer Service URL from the table below**
- Sign on URL: **Please copy the URL from the table below. This will be available once you create the SSO configuration.**

Create

This SAML SSO Configuration is private to your login.

4. On the **SAML SSO Configuration** page, perform the following steps:

## SAML SSO Configuration

Create your SAML 2.0 SSO configuration here.

Copy the mapping values from Azure AD Single sign on Page and then paste it here.

<b>Login URL*</b>	<input type="text" value="https://login.microsoftonline.com/&lt;Tenant ID&gt;/saml2"/>
<b>Azure AD Identifier*</b>	<input type="text" value="https://sts.windows.net/&lt;Tenant ID&gt;/"/>
<b>Logout URL*</b>	<input type="text" value="https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0"/>
<b>Certificate RAW*</b>	<div>Choose File</div>

Create

[Back](#)

- In the **Login URL** textbox, paste the **Login URL** value, which you have copied from the Azure portal.
- In the **Azure AD Identifier** textbox, paste the **Azure AD Identifier** value, which you have copied from the Azure portal.
- In the **Logout URL** textbox, paste the **Logout URL** value, which you have copied from the Azure portal.
- Click **Choose File** and upload the **Certificate (Raw)** file which you have downloaded from the Azure portal.
- Click **Create**.

- f. Copy Sign-on URL, Identifier and ACS URL values on SAML Toolkit SSO configuration page and paste into respected textboxes in the **Basic SAML Configuration** section in the Azure portal.

## Create Azure AD SAML Toolkit test user

In this section, a user called B.Simon is created in Azure AD SAML Toolkit. Please create a test user in the tool by registering a new user and provide all the user details.

## Test SSO

In this section, you test your Azure AD single sign-on configuration with following options.

- Click on **Test this application** in Azure portal. This will redirect to Azure AD SAML Toolkit Sign-on URL where you can initiate the login flow.
- Go to Azure AD SAML Toolkit Sign-on URL directly and initiate the login flow from there.
- You can use Microsoft My Apps. When you click the Azure AD SAML Toolkit tile in the My Apps, this will redirect to Azure AD SAML Toolkit Sign-on URL. For more information about the My Apps, see [Introduction to the My Apps](#).

## Next steps

Once you configure Azure AD SAML Toolkit you can enforce session control, which protects exfiltration and infiltration of your organization's sensitive data in real time. Session control extends from Conditional Access. [Learn how to enforce session control with Microsoft Cloud App Security](#).

## Recommended content

### [Azure Single Sign On SAML Protocol - Microsoft identity platform](#)

This article describes the Single Sign-On (SSO) SAML protocol in Azure Active Directory

## How the Microsoft identity platform uses the SAML protocol

This article provides an overview of the single sign-on and Single Sign-Out SAML profiles in Azure Active Directory.

## SAML authentication with Azure Active Directory

Architectural guidance on achieving SAML authentication with Azure Active Directory

## Troubleshoot SAML-based single sign-on - Azure AD

Troubleshoot issues with an Azure AD app that's configured for SAML-based single sign-on.

## Azure Single Sign Out SAML Protocol

This article describes the Single Sign-Out SAML Protocol in Azure Active Directory

## Tutorial: Azure Active Directory integration with SAML SSO for Confluence by resolution GmbH

Learn how to configure single sign-on between Azure Active Directory and SAML SSO for Confluence by resolution GmbH.

## Configure a SAML 2.0 provider for portals with Azure AD - Power Apps

Learn how to configure SAML 2.0 for portals with Azure Active Directory.

## Quickstart: Enable single sign-on for an enterprise application - Azure AD

Enable single sign-on for an enterprise application in Azure Active Directory.

Show more ▾