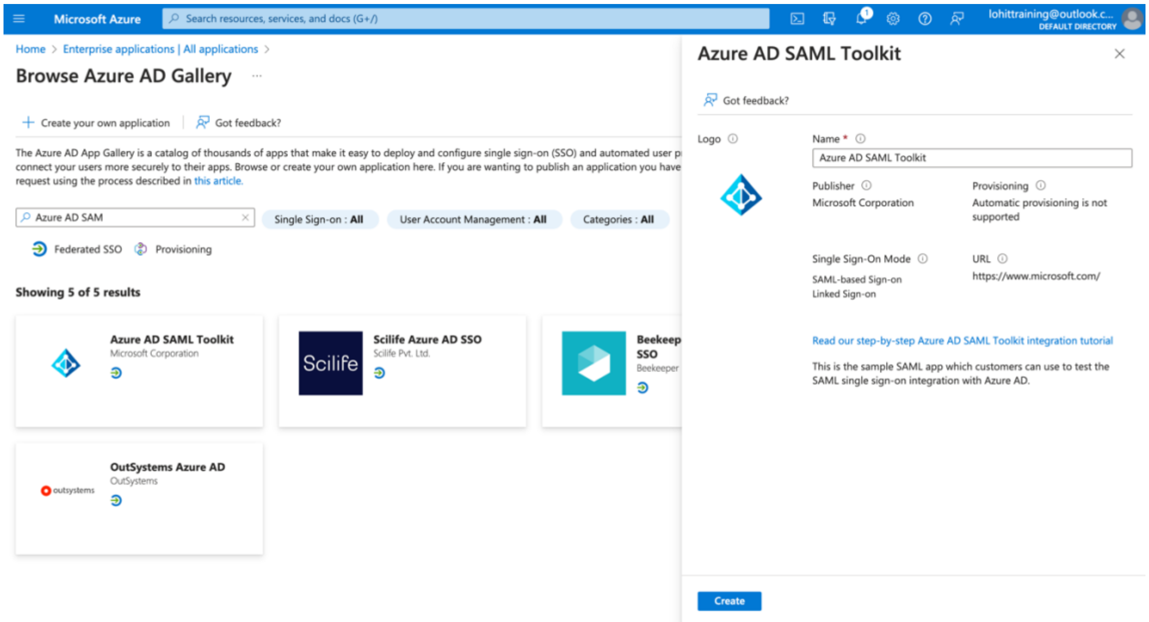
Setting up SSO using Azure Portal

Step 1: I Navigated to Enterprise Application and create a new application. Now search for "**Azure AD SAML Toolkit**". This is Azure application allows us to create Single Sign On's for the users or groups.



The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user p connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have request using the process described in this article.

Azure AD SAM

Showing 5 of 5 results

Azure AD SAML Toolkit
Microsoft Corporation

Azure AD SAML Toolkit

Name * : Azure AD SAML Toolkit

Publisher: Microsoft Corporation

Provisioning: Automatic provisioning is not supported

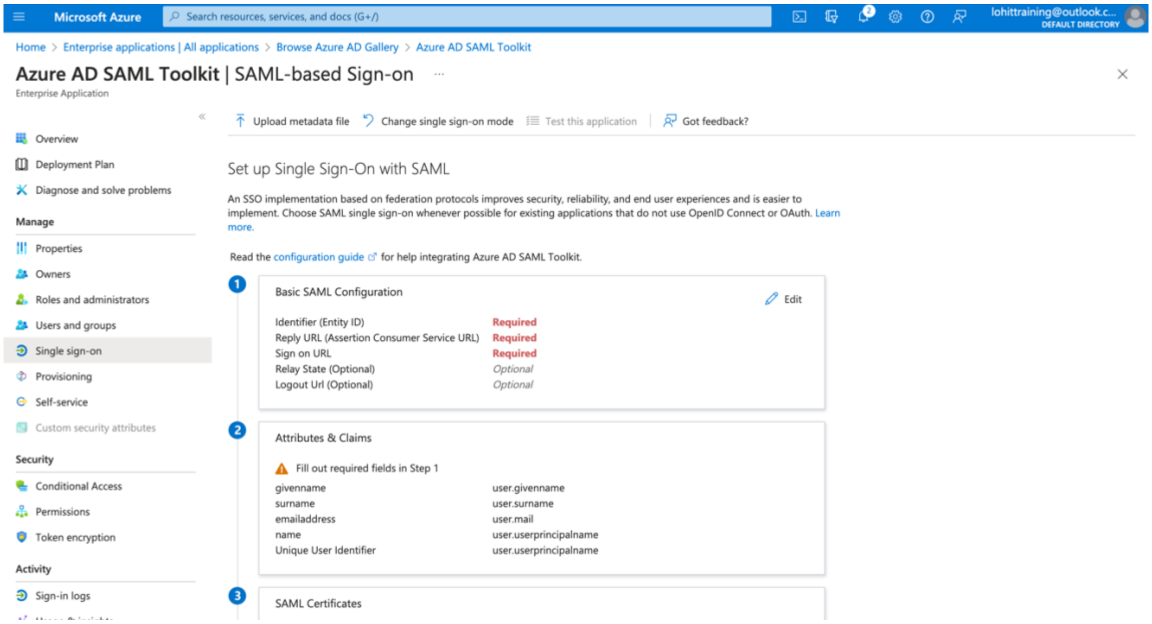
Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://www.microsoft.com/

Read our step-by-step Azure AD SAML Toolkit integration tutorial

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Azure AD.

Step 2: Once the application is created, I started to configure the now create application for Single sign on. You will also have an option to disable SSO or to link an application depending on your need. But I chose SSO.



Azure AD SAML Toolkit | SAML-based Sign-on

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Azure AD SAML Toolkit.

1 Basic SAML Configuration

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

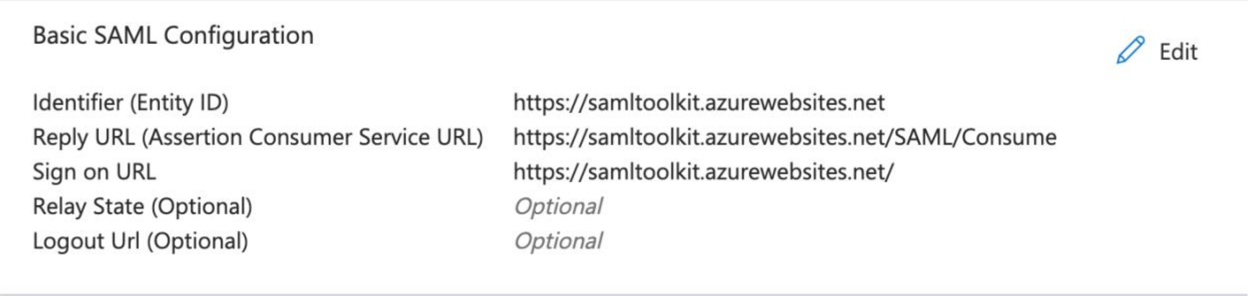
2 Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Step 3: I started off with the basic SAML configuration in which three following fields needed to be configured. First of which was Identifier ID, which was automatically filled for me with *https://samltoolkit.azurewebservices.net*. This is the unique ID that will be used to identify my application. Second, the reply url which is where the application expects to receive authentication tokens from. *https://samltoolkit.azurewebservices.net/SAML/Consume*. Finally the sign on url which is the sign in page for my application and I configured it with *https://samltoolkit.azurewebservices.net*.

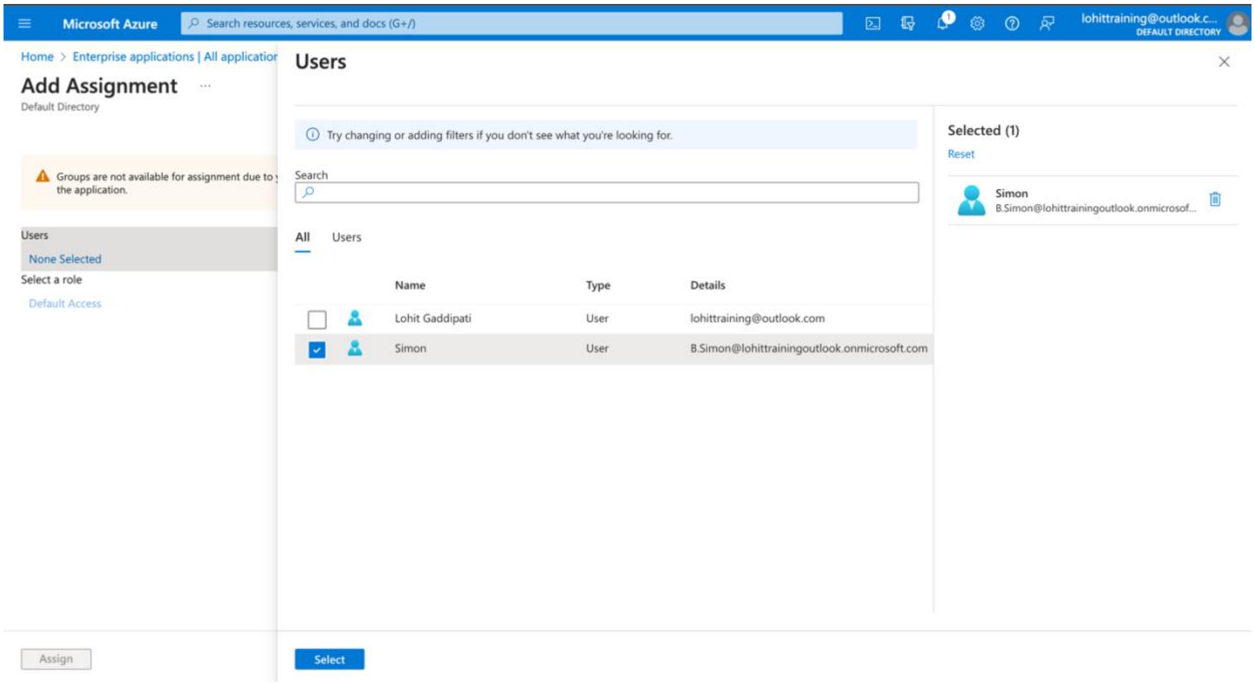


Basic SAML Configuration

Identifier (Entity ID)	https://samltoolkit.azurewebsites.net
Reply URL (Assertion Consumer Service URL)	https://samltoolkit.azurewebsites.net/SAML/Consume
Sign on URL	https://samltoolkit.azurewebsites.net/
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

Step 4: Now, I closed the basic configuration and, on the home, downloaded the raw certificate for future use. Along with which I also copied the following url's
Login url: https://login.microsoftonline.com/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/saml2
Azure AD identifier: https://sts.windows.net/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/
Logout url: https://login.microsoftonline.com/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/saml2

Step 5: Now, I needed to assign user to this. This was done by using *User and Groups* option on the left panel. Now using Add user or group I selected people I needed to add to the application.



Microsoft Azure
Search resources, services, and docs (G+/)
lohittraining@outlook.c...
DEFAULT DIRECTORY
Home > Enterprise applications | All applicatior
Add Assignment
Default Directory
Users
Select
Assign

Groups are not available for assignment due to y the application.

Users
None Selected
Select a role
Default Access

Try changing or adding filters if you don't see what you're looking for.

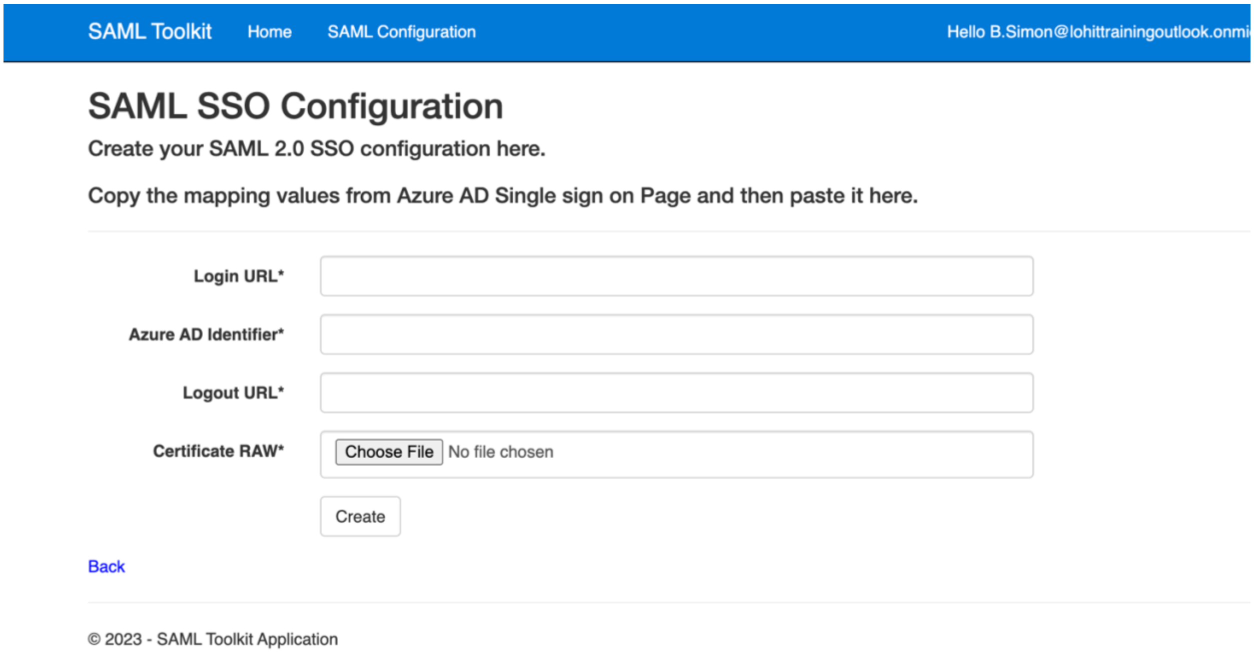
Search

All Users

	Name	Type	Details
□	Lohit Gaddipati	User	lohittraining@outlook.com
☑	Simon	User	B.Simon@lohittrainingoutlook.onmicrosoft.com

Selected (1)
Reset
Simon
B.Simon@lohittrainingoutlook.onmicrosof...

Step 5: Now, On the login page of SAML Toolkit, I logged in and started to configure the application itself. This is where we use all the information that we copied earlier including the raw certificate that we downloaded.



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.

Login URL*

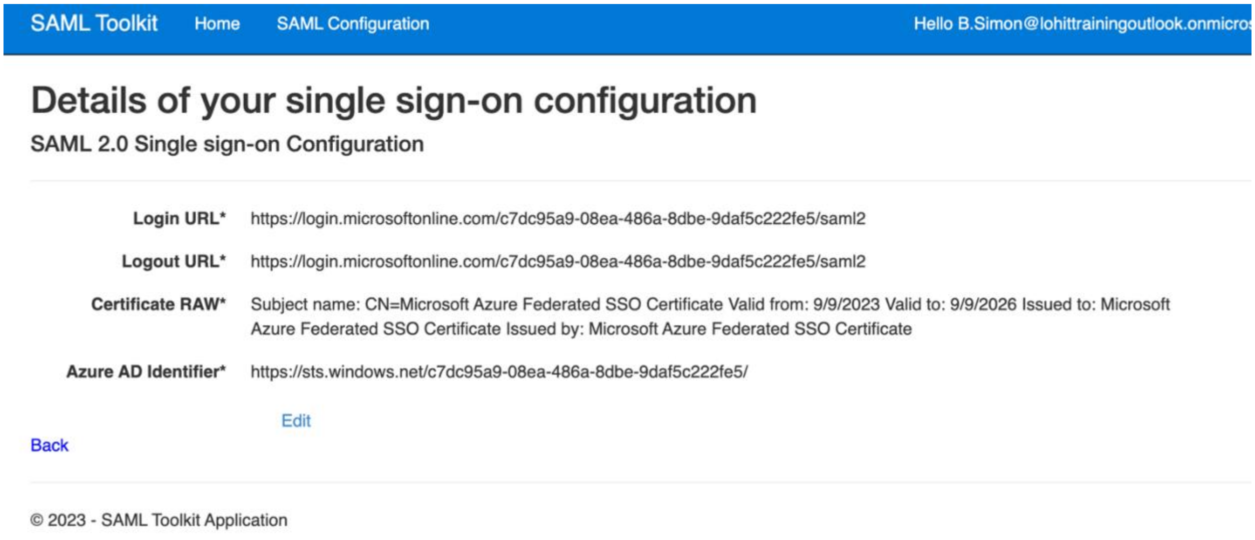
Azure AD Identifier*

Logout URL*

Certificate RAW* No file chosen

© 2023 - SAML Toolkit Application

Step 6: Now, I copied the following information displayed on the page which would be needed for the next steps in configuring the SAML.
SP Initiated Login URL: https://samltoolkit.azurewebsites.net/SAML/Login/13726
Azure AD Identifier: https://sts.windows.net/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/



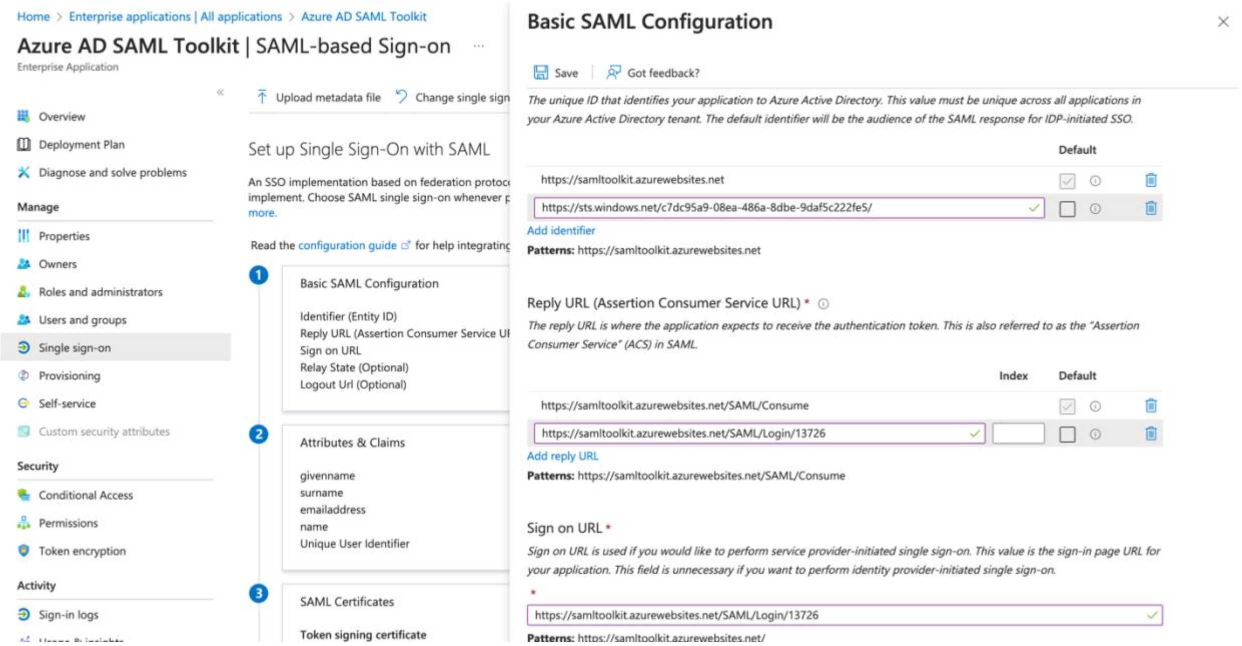
Details of your single sign-on configuration

SAML 2.0 Single sign-on Configuration

Login URL*	https://login.microsoftonline.com/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/saml2
Logout URL*	https://login.microsoftonline.com/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/saml2
Certificate RAW*	Subject name: CN=Microsoft Azure Federated SSO Certificate Valid from: 9/9/2023 Valid to: 9/9/2026 Issued to: Microsoft Azure Federated SSO Certificate Issued by: Microsoft Azure Federated SSO Certificate
Azure AD Identifier*	https://sts.windows.net/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/

© 2023 - SAML Toolkit Application

Step 7: Now in my azure portal, I started making a few changes to the basic configuration. I added a new identifier url and used the above saved sp initiated login url and also added another identifier for the reply url along with sign on url using the azure ad identifier.



An SSO implementation based on federation protoc implement. Choose SAML single sign-on whenever p more.

Read the configuration guide for help integrating

Basic SAML Configuration

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://samltoolkit.azurewebsites.net	☑
https://sts.windows.net/c7dc95a9-08ea-486a-8dbe-9daf5c222fe5/	□

Add identifier

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://samltoolkit.azurewebsites.net/SAML/Consume		☑
https://samltoolkit.azurewebsites.net/SAML/Login/13726		□

Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

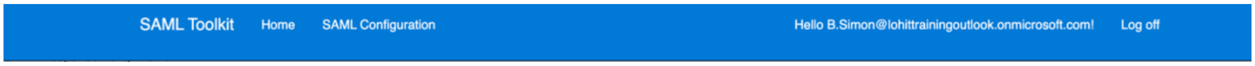
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

https://samltoolkit.azurewebsites.net/SAML/Login/13726

Patterns: https://samltoolkit.azurewebsites.net/

Step 8: Now all that's left was to test the application and I was logged in directly without a verification request which is the purpose of using sso.



Enabling Multi Factor Authentication for users using cloud

Step 1: I started by making sure the security defaults are disabled in properties.

Step 2: I navigated to condition access from security in the left panel and created a new policy

Step 3: Now, I needed to configure a new conditional policy for users or groups. Also, I changed the settings that MFA would be prompted for all the cloud application for the user/group.

Step 4: Finally, I granted the access for multi factor authentication and save the policy and test it.