# SSO Specifications for SAML with Windows® Azure®

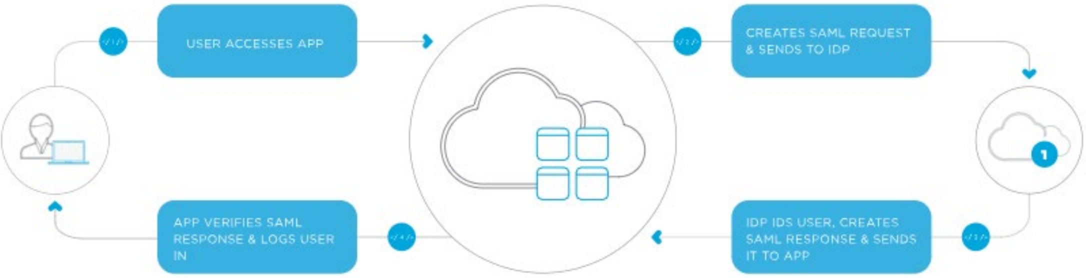
May 27, 2022

## Introduction

SAML SSO works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.

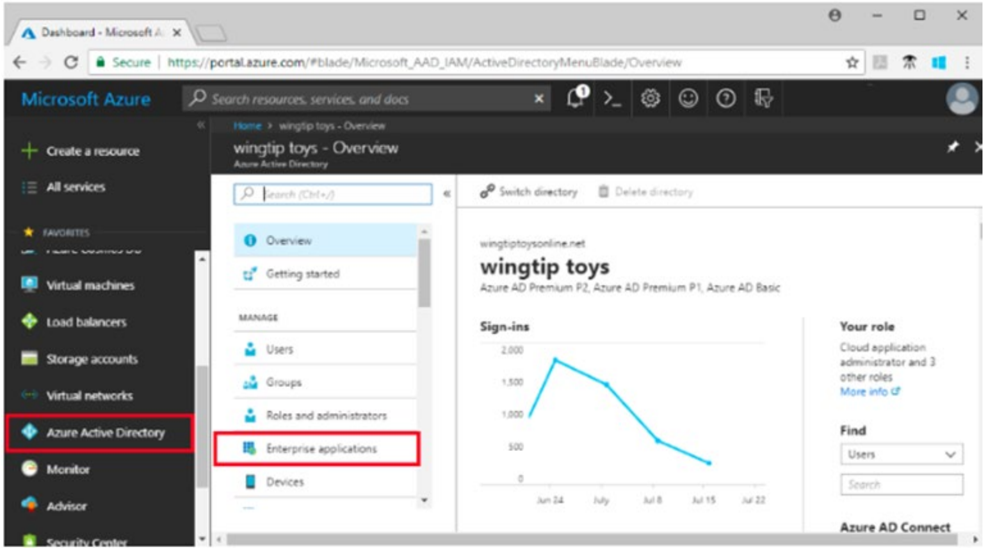
## SAML SSO Flow

The diagram below illustrates the single sign-on flow for service provider-initiated SSO, i.e. when an application triggers SSO.


USER ACCESSES APP
CREATES SAML REQUEST & SENDS TO IDP
IDP IDS USER, CREATES SAML RESPONSE & SENDS IT TO APP
APP VERIFIES SAML RESPONSE & LOGS USER IN

## Add Application to Azure AD Tenant

1. In the Azure portal, on the left navigation panel, click **Azure Active Directory**.
2. In the **Azure Active Directory** blade, click **Enterprise applications**.



3. The All applications blade opens to show a random sample of the applications in your Azure AD tenant.
4. Click **New application** at the top of the **All applications blade**.
5. To search for the application to add, under **Add from the gallery**, enter the name of the application. Select the application from the results and click **Add**.

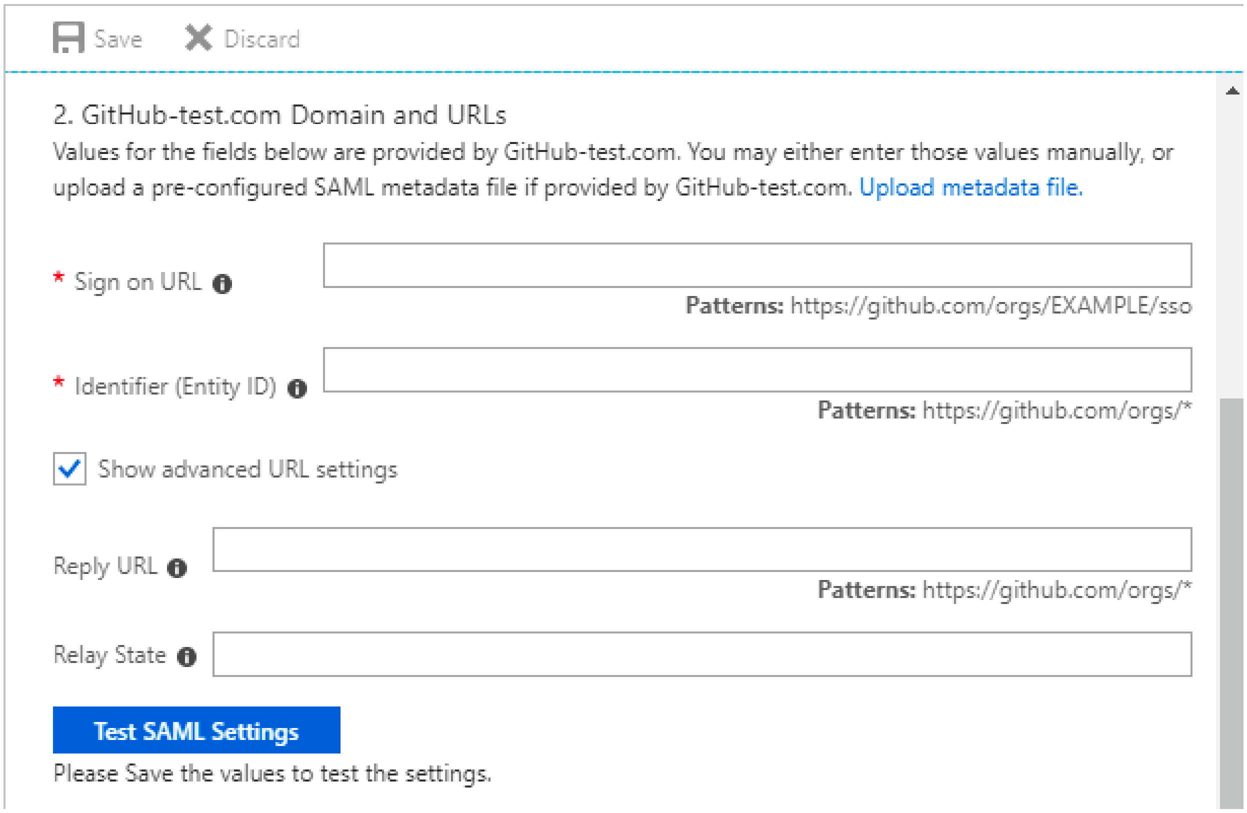
## Configure Domain and URLs

The application vendor must receive the correct information for the following settings:

| Configuration setting | Service Provider-Initiated | Identify Provider-Initiated | Description |
|---|---|---|---|
| Sign-on URL | Required | Required | When a user opens this URL, the service provider redirects to Azure AD to authenticate and sign on the user. Azure AD uses the URL to start the application from Office 365 and the Azure AD Access Panel. When blank, Azure AD performs IDP-initiated single sign-on when a user launches the application from Office 365, the Azure AD Access Panel, or from the Azure AD single sign-on URL. |
| Identifier (Entity ID) | Optional | Required | Uniquely identifies the application for which single sign-on is being configured. Azure AD sends the identifier back to the application as the Audience parameter of the SAML token, and the application is expected to validate it. This value also appears as the Entity ID in any SAML metadata provided by the application. |
| Reply URL | Optional | Required | Specifies where the application expects to receive the SAML token. The reply URL is also referred to as the Assertion Consumer Service (ACS) URL. |

| Configuration setting | Service Provider-Initiated | Identify Provider-Initiated | Description |
|---|---|---|---|
| Relay State | Optional | Optional | Specifies to the application where to redirect the user after authentication is completed. Typically, the value is a valid URL for the application, however some applications use this field differently. For more information, ask the application vendor. |

Select the **Show advanced URL Settings** check box to see all settings. Enter the information and click **Save**.



2. GitHub-test.com Domain and URLs

Values for the fields below are provided by GitHub-test.com. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by GitHub-test.com. Upload metadata file.

* Sign on URL

Patterns: https://github.com/orgs/EXAMPLE/sso

* Identifier (Entity ID)

Patterns: https://github.com/orgs/*

☑ Show advanced URL settings

Reply URL

Patterns: https://github.com/orgs/*

Relay State

Please Save the values to test the settings.

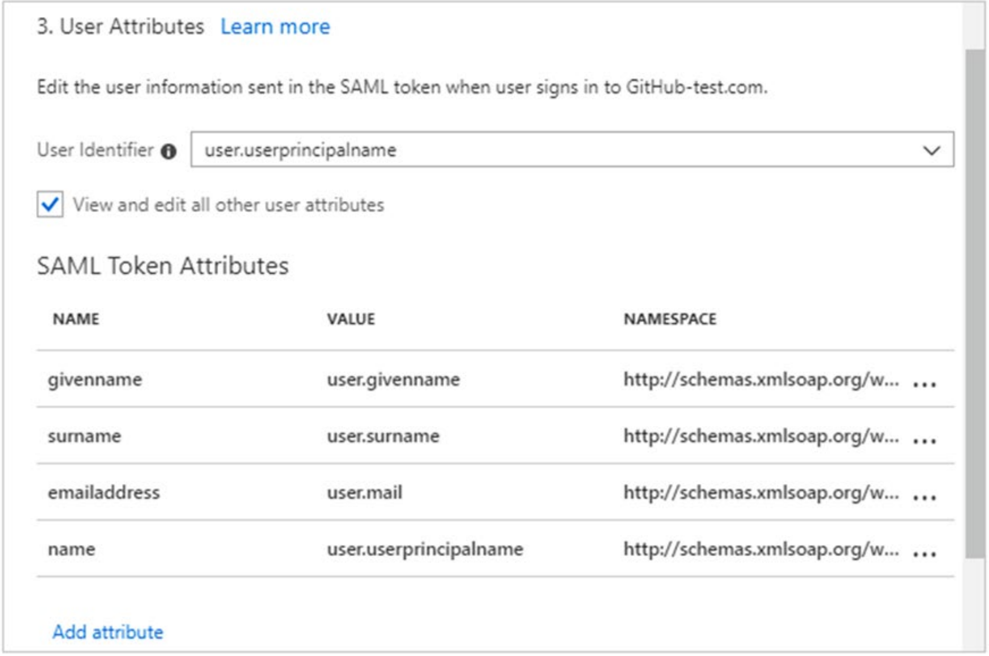
## Configure User Attributes

User attributes allow to control what information Azure AD sends to the application. For example, Azure AD could send the name, email, and employee ID of the user to the application. Azure AD sends the user attributes to the application in the SAML token each time a user signs-in.

These attributes may be required or optional to make single sign-on work properly. For more information, see the application-specific tutorial, or ask the application vendor.

1. Select the **View and edit all other user attributes** check box.

1. To view all the options, click **View and edit all other user attributes**.



3. User Attributes Learn more

Edit the user information sent in the SAML token when user signs in to GitHub-test.com.

User Identifier: user.userprincipalname

☑ View and edit all other user attributes

SAML Token Attributes

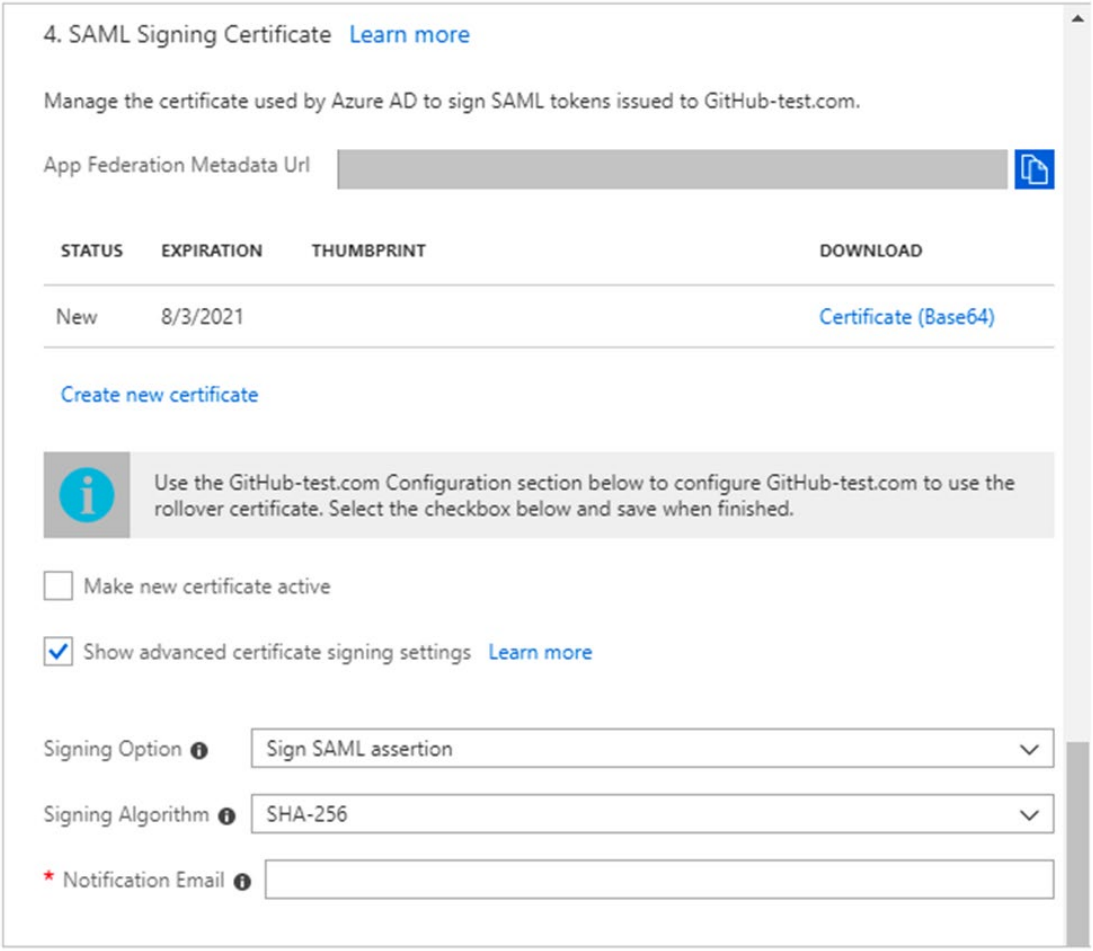
| NAME | VALUE | NAMESPACE |
|---|---|---|
| givenname | user.givenname | http://schemas.xmlsoap.org/w... |
| surname | user.surname | http://schemas.xmlsoap.org/w... |
| emailaddress | user.mail | http://schemas.xmlsoap.org/w... |
| name | user.userprincipalname | http://schemas.xmlsoap.org/w... |

2. Enter the **User Identifier**. The user identifier uniquely identifies each user within the application. For example, if the email address is both the username and the unique identifier, set the value to user.mail.
3. To add an attribute to the SAML Token Attributes, click **Add attribute**. Enter the **Name** and select the **Value** from the menu.
4. Click **Save**.

### Create a SAML Signing Certificate

Azure AD uses a certificate to sign the SAML tokens that it sends to the application.

1. To see all the options, select the **Show advanced certificate signing options** check box.



4. SAML Signing Certificate Learn more

Manage the certificate used by Azure AD to sign SAML tokens issued to GitHub-test.com.

App Federation Metadata Url

| STATUS | EXPIRATION | THUMBPRINT | DOWNLOAD |
|---|---|---|---|
| New | 8/3/2021 | | Certificate (Base64) |

Create new certificate

Use the GitHub-test.com Configuration section below to configure GitHub-test.com to use the rollover certificate. Select the checkbox below and save when finished.

☐ Make new certificate active

☑ Show advanced certificate signing settings Learn more

Signing Option: Sign SAML assertion

Signing Algorithm: SHA-256

* Notification Email:

2. To configure a certificate, click **Create new certificate**.
3. In the **Create New Certificate** blade, set the expiration date, and click **Save**.
4. Select the **Make new certificate active** check box.
5. Click **Save** at the top of the **Single sign-on** blade.

## Assign Users to the Application

To assign a user or group to the application:

1. Open the application in the portal, if it is not already open.
2. In the left application blade, click **Users and groups**.
3. Click **Add user**.
4. In the **Add Assignment** blade, click **Users and groups**.
5. To find a specific user, type the user name into the **Select** box, click the checkbox next to the user's profile photo or logo, and click **Select**.
6. Find current username and select it.
7. In the **Add Assignment** blade, click **Assign**. When completed, the selected users appear in the **Users and groups** list.

### Configure the application to use Azure AD

As a final step, the applications needs to be configured to use Azure AD as a SAML identity provider.

1. Scroll down to the end of the **Single sign-on** blade for application.
2. Click **Configure application** in the portal and follow the instructions.
3. Manually create user accounts in the application for the purpose of testing single sign-on. Create the user accounts you assigned to the application in the previous section.

### Test Single Sign-On

1. Open the single sign-on settings for application.
2. Scroll to the **Configure domain and URLs** section.
3. Click **Test SAML Settings**. The testing options appear.