SAML v2.0 SSO with Entra ID - Integration Guide

Field	Details
Document Type	How-To Guide: SSO Integration
Applies To	Microsoft Entra ID, Any SAML 2.0-compatible SaaS or Third-Par Application
Audience	2nd Line / Systems Administrator / IT Engineer
Author	AK. Udofeh
Last Updated	March 2026

Overview

This article covers how to configure Single Sign-On (SSO) using the SAML 2.0 protocol between Microsoft Entra ID and any third-party or SaaS application that supports SAML for authentication. It is intended for systems administrators who need to integrate enterprise applications with Entra ID to centralise identity management, enforce MFA, and control user access. The guide covers Enterprise Application creation in Entra ID, SAML endpoint configuration, certificate handling, and attribute claim mapping.

SAML SSO works by delegating authentication to Entra ID as the Identity Provider (IdP). The application (Service Provider / SP) redirects the user to Entra's SAML endpoint, which authenticates the user and returns a signed SAML assertion containing identity attributes. The application validates the assertion signature using Entra's signing certificate and establishes a user session.

Common Failure Points

- Incorrect ACS (Assertion Consumer Service) URL registered in Entra
- Entity ID mismatch between the application and Entra configuration
- Entra signing certificate not imported into the application, or certificate has expired
- Attribute claims not mapping to the fields the application expects
- SLO (Single Logout) URL misconfigured, causing logout failures
- User not assigned to the Enterprise Application in Entra

Before You Start

Check	Where
You have Global Administrator or Application Administrator rights in Entra ID	Entra ID > Roles and Administrators
The target application supports SAML 2.0 (not only OIDC)	Application vendor documentation
You have the application's ACS URL, Entity ID, and SLO URL	Application vendor documentation or SP metadata XML
Outbound HTTPS (port 443) from the application server to login.microsoftonline.com is permitted	Firewall / network policy

You have admin access to the application's configuration	Application admin console or hosting environment

Step 1: Create an Enterprise Application in Entra ID

> For SAML SSO, configuration is done through Enterprise Applications, not App Registrations. An App Registration is created automatically in the background.

- Navigate to portal.azure.com > Entra ID > Enterprise Applications > New application.
- Click Create your own application.
- Enter a display name (e.g. AppName SAML SSO).
- Select "Integrate any other application you don't find in the gallery".
- Click Create.

> You will be taken to the application overview page.

Step 2: Configure SAML Settings

- Inside the Enterprise Application, go to Single Sign-On > SAML.
- Click Edit on the Basic SAML Configuration panel.
- Fill in the following fields using values from your application's documentation or SP metadata:

Identifier (Entity ID)*: https://app.yourdomain.com/saml/metadata
(this is a Unique URI that identifies the Service Provider)

Reply URL (Assertion Consumer Service URL)*: https://app.yourdomain.com/saml/acs
(this is where Entra ID posts the signed SAML assertion)

Sign-on URL (optional): https://app.yourdomain.com/login
(SP-initiated login entry point)

Logout URL (optional): https://app.yourdomain.com/saml/sls
(SP's Single Logout endpoint)

> If the application provides a metadata XML URL (e.g. https://app.yourdomain.com/saml/metadata), Entra can import these values automatically — click Upload metadata file at the top of the Basic SAML Configuration panel.
>
> Click Save.

Step 3: Download the Entra Signing Certificate

- Still in the SAML configuration view, scroll to Section 3 > SAML Certificates.
- Download Certificate (Base64) > this produces a .cer or .pem file.

- Open the file in a text editor. The content between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- is the base64-encoded certificate value you will need for the application.

> Store a copy of this certificate securely. If Entra's signing certificate is rotated (e.g. on expiry), the application will fail to validate assertions until the new certificate is imported.

Step 4: Collect IdP Configuration Values

In the SAML configuration page, note the following values in the "Set up <app name>":

Value	Description
Login URL	Entra's SAML SSO endpoint - set as the IdP SSO URL in the appli
Logout URL	Entra's SAML SLO endpoint - set as the IdP SLO URL in the appl
Entra ID Identifier	Entra's Entity ID - set as the IdP Entity ID in the application
Certificate (Base64)	Signing certificate from Step 3 - used by the application to validate assertions

Alternatively, download the Federation Metadata XML from the same section - many applications can import this file directly to auto-populate all IdP settings.

Step 5: Configure Attribute Claims in Entra

By default, Entra sends a standard set of SAML attribute claims. Verify these match what the application expects:

- In the Enterprise Application SAML configuration, click Edit on Section 2 - Attributes & Claims.

The default claims sent by Entra are:

Claim Name	**Value**
emailaddress	user.mail
givenname	user.givenname
surname	user.surname
name	user.userprincipalname

- If the application requires different attribute names or additional claims, click Add new claim to add or rename them.
- To include group membership in the assertion (for role mapping), click Add a group claim > select Security groups.

> By default, Entra sends group Object IDs (GUIDs) in the group claim, not display names. Configure the application's role mapping to use Object IDs, or change the group claim's source attribute to display names if supported.

Step 6: Restrict Access via Enterprise Application (Recommended)

- - In the Enterprise Application, go to Properties.
  - Set "Assignment required?" to Yes > Save.

- Go to Users and groups > Add user/group > assign the relevant users or Entra security groups.

> Only assigned users will be permitted to authenticate via SAML SSO. Unassigned users receive an Entra-side access denied error before reaching the application.

Step 7: Configure the Application

In the Service Provider application, enter the values collected in Step 4 into the application's SAML configuration. The exact setting names vary per application - refer to the application vendor's SAML documentation. The standard SAML parameters are:

Application Setting	Value to Enter
IdP Entity ID	Entra ID Identifier from Step 4
IdP SSO URL	Login URL from Step 4
IdP SLO URL	Logout URL from Step 4
IdP X.509 Certificate	Certificate base64 content from Step 3
SP Entity ID	Must match the Identifier (Entity ID) entered in Entra Step 2
ACS URL	Must match the Reply URL entered in Entra Step 2
Name ID Format	emailAddress or persistent - check application documentation
Binding	HTTP-POST for ACS; HTTP-Redirect for AuthnRequest

==========Troubleshooting==========

AADSTS750054: SAMLRequest or SAMLResponse must be present as query string parameters

Cause: The application is not correctly forming the SAML AuthnRequest, or the binding type does not match Entra's expectation.
Resolution:

- Confirm the application is using HTTP Redirect binding for the AuthnRequest - Entra requires this for SP-initiated flows.
- Check the application's SAML configuration for a "request binding" or "binding type" setting and ensure it is set to HTTP-Redirect.

AADSTS70011: The provided value for the input parameter 'redirect_uri' is not valid

Cause: The ACS URL registered in Entra does not match the URL the application is posting to.
Resolution:

- Retrieve the application's SP metadata from its metadata URL or admin panel.
- Compare the AssertionConsumerService URL in the metadata against the Reply URL (ACS URL) registered in Entra.
- Update the Reply URL in Entra to match exactly - including scheme (https://), full path, and no trailing slash.

AADSTS750057: Invalid SAML response or no SAML response

Cause: The Entity ID in the application does not match what is registered in Entra, or the SAML response is malformed.

Resolution:

- Confirm the SP Entity ID configured in the application exactly matches the Identifier (Entity ID) in Entra.
- Confirm the IdP Entity ID configured in the application matches the Entra ID Identifier shown in Section 4 of the Entra SAML page.
- These values are case-sensitive and must match character for character.

Assertion signature validation fails / Invalid signature

Cause: The X.509 certificate used for validation in the application does not match the current Entra signing certificate, or the certificate has expired.

Resolution:

- In the Enterprise Application SAML configuration > Certificates > check the expiry date of the active certificate.
- If expired or rotated, click New Certificate, make it active, and download the new Base64 certificate.
- Import the new certificate into the application's SAML configuration.
- Restart the application service if required.

> Entra signing certificates expire every 3 years by default. Set a calendar reminder 60 days before expiry to plan a rotation window.

Single Logout (SLO) does not work - user remains signed in to Entra after signing out of the application

Cause: The SLO URL is not configured in either Entra or the application, or the binding types do not match.

Resolution:

- Confirm the Logout URL field in Entra's Basic SAML Configuration points to the application's SLO endpoint.
- Confirm the application's IdP SLO URL is set to the Logout URL shown in Entra Section 4.
- Entra uses HTTP Redirect binding for logout requests - confirm the application's SLO endpoint accepts GET/Redirect binding, not only POST.

User authenticates successfully in Entra but receives an error or no access in the application

Cause: The SAML assertion was accepted, but the user account was provisioned with no role or permissions in the application.

Resolution:

- Log in to the application as an administrator.
- Assign an appropriate role to the SSO-provisioned user account.
- To automate this for future users, configure a default role for SSO-registered accounts, or implement group-to-role mapping using the group claim configured in Step 6.

Attribute claims are empty or not recognised by the application

Cause: The attribute claim names sent by Entra do not match the names the application is expecting.
Resolution:

- In Entra ? Enterprise Application > Attributes & Claims, note the full claim URI names being sent (e.g. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress).
- Cross-reference these with the application's expected attribute names from the vendor documentation.
- Either rename claims in Entra to match the application, or update the application's attribute mapping to match Entra's output.
- Use a SAML tracer browser extension or the application's debug mode to inspect the raw assertion during a test login.

Expected Outcome

Factor	Detail
Resolution Time	45–90 minutes for initial configuration; additional time if attribute requires investigation
User Impact	Zero - SAML SSO is additive; existing local accounts remain func during migration
Recurrence Risk	Low - primary recurring issue is Entra signing certificate expiry (e years by default)
Ongoing Maintenance	Rotate Entra signing certificate before expiry; manage user access Enterprise Application assignments

Revision #6
Created 2026-03-05 17:29:38 UTC by AK. Udofeh
Updated 2026-03-19 10:15:12 UTC by AK. Udofeh