State of Maine Identity Provider (IdP) settings

|  |  |
| --- | --- |
| **Element** | **Configuration Value** |
| Identity provider issuer | https://sts.windows.net/413fa8ab-207d-4b62-9bcd-ea1a8f2f864e/ |
| Identity provider login URL | https://login.microsoftonline.com/413fa8ab-207d-4b62-9bcd-ea1a8f2f864e/saml2 |
| Identity provider logout URL | https://login.microsoftonline.com/413fa8ab-207d-4b62-9bcd-ea1a8f2f864e/saml2 |

Application Owner Responsibility

* Fill out information below and email to EnterpriseDirectoryServices@StateOfMaine.onmicrosoft.com
* Questions? Contact EnterpriseDirectoryServices@StateOfMaine.onmicrosoft.com

Required Partner Information:

|  |  |
| --- | --- |
| **Project / Application Function** |  |
| Description*Provide the summary of what this application does.* * *Is this application for POC or Production use?*
 |  |
| Platform*Provide a description of the application platform**ACS federation requests**Applications which need ACS federations for service bus/caching service etc. are allowed and any other ACS tenant request needs to be onboarded to the Service Provider (SP) tenant or STS.maine.gov directly.* | Examples**:**xbxcACSADFSv2ADFSv3ADFSv4ShibbolethAzure applicationSharePoint 2010 siteThird-party STS [*Specify product name*] |
| **Sponsor Details** |  |
| Service Provider Sponsor Alias |  |
| Vendor Contact Information*For vendor or third-party developed applications* | Name:Email:Company:Phone: |

SAML-based single sign-on

|  |  |
| --- | --- |
| **Basic SAML Configuration** |  |
| Identifier (Entity ID) \*requiredThe default identifier will be the audience of the SAML response for IDP-initiated SSO | Example:https://app.knowledgeowl.com/sphttps://app.knowledgeowl.com/sp/id/<unique ID> |
| Reply URL (Assertion Consumer Service URL) \*requiredThe default reply URL will be the destination in the SAML response for IDP-initiated SSO | Example:https://subdomain.knowledgeowl.com/home/saml-loginhttps://privatedomain.com/home/saml-login |
| Sign on URLThis URL contains the sign-in page for this application that will perform the service provider-initiated single sign-on. Leave it blank if you want to perform identity provider initiated single sign-on. | Example:https://subdomain.knowledgeowl.com/home/saml-loginhttps://privatedomain.com/home/saml-login |
| Relay StateOptionally, a SAML RelayState parameter can be provided. The RelayState instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application. The value in this form only takes effect in an IdP-initiated SSO flow. If your application uses SP-initiated SSO, then the service provider needs to send the RelayState as a parameter in the SAML request. | Optional |
| Logout URLThis URL is used to send the SAML Logout response back to the application. | Optional |

Note: Line-of-business apps that use OAuth 2.0, OpenID Connect, or WS-Federation can be integrated with Azure AD as app registrations.

Default User Attributes & Claims

|  |  |
| --- | --- |
| **Required Claim** |  |
| Claim name | Value |
| Unique User Identifier (Name ID) | user.userprincipalname [nameid-format:emailAddress] |

|  |  |
| --- | --- |
| **Additional Claims** |  |
| Claim name | Value |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | user.mail |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | user.givenname |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | user.userprincipalname |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | user.surname |

Requested Claims

|  |  |
| --- | --- |
| Specify the Claims/assertions your application will consumeNotes:‘tokenGroups’ will not be issued; individual group names will be emitted as Group or Role claims | **Examples:*** Email
* UPN
* FirstName
* LastName
* EmployeeId
* etc.
 |

Authorization Rules

|  |  |
| --- | --- |
| Specify rules to permit or deny a user or group of users to receive a SAML token for this relying party. The default Authorization Rule for new Relying Parties is “Deny All” – all authorization logic must be specified by the RP owner. | **Examples:*** Permit all users
* Permit only users belonging to security group “SOM\Foo” (all others will be denied by default)
 |

Token Encryption

|  |  |
| --- | --- |
| Require Token Encryption | Yes/No |

SAML Signing Certificate

|  |  |
| --- | --- |
| Certificate format | Base-64 .cer or RAW |

Certificate signing algorithms

Azure AD supports two signing algorithms, or secure hash algorithms to sign the SAML response: SHA256 and SHA1.

|  |  |
| --- | --- |
| Support for SHA256 | Yes/No \* if No, an exemption will be needed for SHA1 |

Last updated: 8/1/2022