SSO Integration using SAML

**Single Sign on (SS0)**

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords,

**Request from Site for Login**

|  |
| --- |
| Domain/prompt.aspx?**SAMLRequest**=jZJNj9owEIbv%2FArkO4nDR8NagEShH0gU0ML20Mtq4gxZS46depwu%2Ffd1kqW73QOqb57x89rv65kRlLoSy9o%2FmXv8WSP5Xj%2BsS6kNibY5Z7UzwgIpEgZKJOGlOC6%2FbcUw4qJy1ltpNXuH3aaACJ1X1nTYZj1n%2B92n7f7LZvfIJ6MsyXEsp%2Bnd6E4C58MJ5zzlYzhzmGYfMB9P0uG5Q7%2Bjo6AzZ0GW9To1oho3hjwYH%\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%2BVyZUpbjvOukMkvp5Oh8Fhfzx1IstrEitrqC7RHdH9UhIf7revj2rfEvwUGFEJWj9bp3MNGUXSlnET9yNIYotWcdbsRRuCW%2FyXwix%2Bi7yKVGIXfGzWB6uV%2FN3Wm%2FXZuhL8bbtNReWDc3tU1IYqlOqsMGd%2FZZZa2%2BeVQ%2FA4Z97VyPrxP5e%2FzCPm7XSGfDxefH8VfgGcoubT8ALSX23HN6hF79p%2BO%2BmLPw%3D%3D&**RelayState**=https%3A%2F%\*\*\*\*\*\*.stage.\*\*\*\*\*.com%2Fhome&**SigAlg**=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&**Signature**=\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Z9e4bgJCbxxGYp3%2FkADbQgr0NfkuwYAPNTan8c4xiNsvOgduIPASDq7ZktJkcX58iZQvvPZogKulB4Q%3D HTTP/1.1 |
| **SAMLRequest** |
| jZJNj9owEIbv%2FArkO4nDR8N\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*9P0uG5Q7%2Bjo6AzZ0GW9To1oho3hjwYH%2Bo8SQcJHyTTE0%2FFKBHD0Y8OXQezyoBv8SfvKxJxTGS1LZSJisxDZF3RVCDEEwenZeUjoOrS8YcX6x%2BVyZUpbjvOukMkvp5Oh8Fhfzx1IstrEitrqC7RHdH9UhIf7revj2rfEvwUGFEJWj9bp3MNGUXSlnET9yNIYotWcdbsRRuCW%2FyXwix%2Bi7yKVGIXfGzWB6uV%2FN3Wm%2FXZuhL8bbtNReWDc3tU1IYqlOqsMGd%2FZZZa2%2BeVQ%2FA4Z97VyPrxP5e%2FzCPm7XSGfDxefH8VfgGcoubT8ALSX23HN6hF79p%2BO%2BmLPw%3D%3D& |
| **RelayState** |
| Redirect URL after login |
| **SigAlg** |
| http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1 |
| **Signature** |
| JEFkLd3haicswpiC3GGwkEzipaasSsYi%2BdAuEQyan8zYF3lJb7p9SyEp3JprA6EtHQirLeDaYI4R5CfCJzbLpBo70OnwoQHaZ9e4bgJCbxxGYp\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*uIPASDq7ZktJkcX58iZQvvPZogKulB4Q%3D |

**Decode Request Format**

|  |
| --- |
| **SamlRequest** |
| jZJNj9owEIbv%2FArkO4nDR8NagEShH0gU0ML20Mtq4gxZS46depwu%2Ffd1kqW73QOqb57x89rv65kRlLoSy9o%2FmXv8WSP5Xj%2BsS6kNibY5Z7UzwgIpEgZKJOGlOC6%2FbcUw4qJy1ltpNXuH3aaACJ1X1nTYZj1n%2B92n7f7LZvfIJ6MsyXEsp%2Bnd6E4C58MJ5zzlYzhzmGYfMB9P0uG5Q7%2Bjo6AzZ0GW9To1oho3hjwYH%2Bo8SQcJHyTTE0%\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%2FZZZa2%2BeVQ%2FA4Z97VyPrxP5e%2FzCPm7XSGfDxefH8VfgGcoubT8ALSX23HN6hF79p%2BO%2BmLPw%3D%3D |
| **Decoded XML** |
| <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  ID="\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"  Version="2.0"  IssueInstant="2017-10-18T07:31:23Z"  Destination="\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  AssertionConsumerServiceURL="\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"  >  <saml:Issuer>https://\*\*\*\*\*\*\*\*\*.com</saml:Issuer>  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified"  AllowCreate="true"  />  <samlp:RequestedAuthnContext Comparison="exact" />  </samlp:AuthnRequest> |

**Ref URL to Decode Request**

|  |
| --- |
| https://www.samltool.com/decode.php |
| <http://phpseclib.sourceforge.net/x509/decoder.php> |
| https://idp.ssocircle.com/sso/toolbox/samlDecode.jsp |

**Receiver**

|  |  |
| --- | --- |
| URL | \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*saml\_acs |
| Parameters | SAMLResponse, RelayState |
|  |  |

|  |
| --- |
| **SAML Response** |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*+Y0tDWUI3YUQ3U0haR2NHbmxORGo2TFIycGE4enJVRGc5citLanNvT01pNEFPRDFuL0J\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*+bWdvbGRlbkBnYnRhLm9yZzwvc2FtbDpBdHRyaWJ1dGVWYWx1ZT48L3NhbWw6QXR0cmlidXRlPjxzYW1sOkF0dHJpYnV0ZSBOYW1lPSJMYXN0TmFtZSIgRnJpZW5kbHlOYW1lPSJHb2xkZW4iPjxzYW1sOkF0dHJpYnV0ZVZhbHVlPkdvbGRlbjwvc2FtbDpBdHRyaWJ1dGVWYWx1ZT48L3NhbWw6QXR0cmlidXRlPjxzYW1sOkF0dHJpYnV0ZSBOYW1lPSJDdXN0b21lcmlkIiBGcmllbmRseU5hbWU9IjU1MTIyNSI+PHNhbWw6QXR0cmlidXRlVmFsdWU+NTUxMjI1PC9zYW1sOkF0dHJpYnV0ZVZhbHVlPjwvc2FtbDpBdHRyaWJ1dGU+PC9zYW1sOkF0dHJpYnV0ZVN0YXRlbWVudD48L3NhbWw6QXNzZXJ0aW9uPjwvc2FtbHA6UmVzcG9uc2U+ |
| **RelayState** |
| Third party URL |

SAML XML Response

|  |
| --- |
| <samlp:Response ID="\_6b5fc4a8-e47d-48a3-a19d-48f142250066"  InResponseTo="\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"  Version="2.0"  IssueInstant="2017-10-18T04:18:55Z"  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"  >  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">\*\*\*\*\*\*\*</saml:Issuer>  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />  <Reference URI="#\_6b5fc4a8-e47d-48a3-a19d-48f142250066">  <Transforms>  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">  <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"  xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"  />  </Transform>  </Transforms>  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  <DigestValue>9gjjKMDDl6xZQ4CXCGVCqt5WzNU=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>\*\*\*\*\* +x4GjmI0TrJfuCHcJlDjj1m00hSM1UBdgp/3RNpy49CVdmonJzRndhpT0oFcwq6V8zB0kfZUeuzeb0aWNw==</SignatureValue>  <KeyInfo>  <X509Data>  <X509Certificate>MIIFTTCCBDWgAwIBAgIIGwk/ +rF0Fw8zDR/iGZjkwDQYJKoZIhvcNAQELBQADggEBAG5FhJtyra1qm4dTSuKplizhxRoq7agPtjkRmzbEXsiIILkuhDWnWiB0/Mm0p3wPkK5r6W8/xfUnRxmxkrDBNZjaCOk+8i1+tH9DBtw2mvf7WhGE4FGM9W+Z6i+W1up7V0G9WPkTlvZn9hfB/h75Zh5b0XdhfSdCapdSfAxzii2EcT7BQV9V3yfyTZHNgZ23nEZ0hIH2C7gunWgA8KQYiRdKdtkgSkyGB3If8j+LsUgOF3Or1Io5gNX4qvvpXk+jxZVWbIBMQ3Eyf67m1TGkZ6tWywKqUstwflmk/RF0wIX81RLAxAZwradaSp6u1wiUo+KhOXrVZbU/xEpLb9UK/l4=</X509Certificate>  </X509Data>  </KeyInfo>  </Signature>  <samlp:Status>  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />  </samlp:Status>  <saml:Assertion Version="2.0"  ID="\_3c6600be-4fa9-4e0c-98c6-de3cbe88c4b3"  IssueInstant="2017-10-18T08:24:20.878Z"  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  >  <saml:Issuer>**\*\*\*\*\*\*\***</saml:Issuer>  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />  <Reference URI="#\_3c6600be-4fa9-4e0c-98c6-de3cbe88c4b3">  <Transforms>  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">  <InclusiveNamespaces PrefixList="#default saml ds xs xsi"  xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"  />  </Transform>  </Transforms>  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  <DigestValue>Y7F7WepS4GDzuvKaEFiivJ5y87Y=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>lTkitwV+PiKXpPLTlfHDA4qNYAG7HOhsz7rwfpsSymKtgVI+3qv2tgCSmfoWfbDus7bMyaHvjjuG79R/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* /h8zLFbzqardg9rB2hiW4iEhWxWtTf96jU5HWt6gZsCJ9gxHG0DMj1elzZ1OZheQYwk8sAZZOQ3nHeP9198m3yQjgG9nfa13LeVUca9vpzPp3O51vIF2WyQdqBdn78/tS3Gnmpsq/BL8/G9CI0Q==</SignatureValue>  <KeyInfo>  <X509Data>  <X509Certificate>MIIFTTCCBDWgAwIBAgIIGwk\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* </X509Certificate>  </X509Data>  </KeyInfo>  </Signature>  <saml:Subject>  <saml:NameID>551225</saml:NameID>  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">  <saml:SubjectConfirmationData NotOnOrAfter="2017-10-23T08:24:20.879Z"  Recipient="https://\*\*\*\*\*\*/saml\_acs"  InResponseTo="ONELOGIN\_\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"  />  </saml:SubjectConfirmation>  </saml:Subject>  <saml:Conditions NotBefore="2017-10-18T08:24:20.879Z"  NotOnOrAfter="2017-10-18T08:29:20.879Z"  />  <saml:AuthnStatement AuthnInstant="2017-10-18T08:24:20.88Z"  SessionIndex="14e8b8e0-0f52-4bd5-bc7f-b8b6f35cfecb"  SessionNotOnOrAfter="2017-10-18T13:24:20.88Z"  >  <saml:AuthnContext>  <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>  </saml:AuthnContext>  </saml:AuthnStatement>  <saml:AttributeStatement>  <saml:Attribute Name="Email"  FriendlyName="mgolden "  >  <saml:AttributeValue>mgolden </saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="FirstName"  FriendlyName="Michael"  >  <saml:AttributeValue>Michael</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="Username"  FriendlyName="mgolden "  >  <saml:AttributeValue>mgolden </saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="LastName"  FriendlyName="Golden"  >  <saml:AttributeValue>Golden</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="Customerid"  FriendlyName="551225"  >  <saml:AttributeValue>551225</saml:AttributeValue>  </saml:Attribute>  </saml:AttributeStatement>  </saml:Assertion>  </samlp:Response> |