# AEM Configuration

|  |  |
| --- | --- |
| Adobe Granite SAML 2.0 Authentication Handler | |
| Path | /content/calix/ Repository path for which this authentication handler should be used by Sling. If this is empty, the authentication handler will be disabled. (path) |
| Service Ranking | 99999 OSGi Framework Service Ranking value to indicate the order in which to call this service. This is an int value where higher values designate higher precedence. Default value is 0. (service.ranking) |
| IDP URL | <https://sfdev2-sfdev2-calixsfdev2.cs12.force.com/Community/idp/login?app=0spV0000000CaXF>  URL of the IDP where the SAML Authentication Request should be sent to. If this property is empty the authentication handler is disabled. (idpUrl) |
| IDP HTTP Redirect | yes  Use an HTTP Redirect to the IDP URL instead of sending an AuthnRequest-message to request credentials. Use this for IDP initiated authentication. (idpHttpRedirect) |
| Service Provider Entity ID | calix-dev-local-poc ID which uniquely identifies this service provider with the identity provider. If this property is empty the authentication handler is disabled. (serviceProviderEntityId) |
| Default Redirect | /content/calix/en/home.html The default location to redirect to after successful authentication. (defaultRedirectUrl) |
| UserID Attribute | userId The name of the attribute containing the user ID used to authenticate and create the user in the CRX repository. Leave empty to use the Subject:NameId. (userIDAttribute) |
| Use Encryption | yes  Whether or not this authentication handler expects encrypted SAML assertions. If this is enabled an RSA key pair must be provided at /etc/key/saml. (useEncryption) |
| Autocreate CRX Users | yes  Whether or not to autocreate nonexisting users in the repository. (createUser) |
| Add to Groups | yes  Whether or not a user should be autmatically added to CRX groups after successful authentication. (addGroupMemberships) |
| Group Membership | groups The name of the attribute containing a list of CRX groups this user should be added to. (groupMembershipAttribute) |
| NameIDPolicy Format | urn:oasis:names:tc:SAML:2.0:nameid-format:persistent The value of the NameIDPolicy format parameter to send in the AuthnRequest message. (nameIdFormat) |
| Synchronized Attributes | A list of attribute mappings (in the format "attributename=path/relative/to/user/node") which should be stored in the repository on user-synchronization. (synchronizeAttributes) |

# Sales Force Configuration – sfdev2

* Salesforce Server: <https://calix--sfdev2.cs30.my.salesforce.com/>
* Credentials: [salesforcesystem@calix.com.sfdev2](mailto:salesforcesystem@calix.com.sfdev2) | salesforce123
* Configuration url: <https://calix--sfdev2.cs12.my.salesforce.com/_ui/core/application/force/connectedapp/ForceConnectedApplicationPage/d?applicationId=06PV00000008PlC>

### SAML Service Provider Settings

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity Id** | calix-dev-localhost-poc | **ACS URL** | http://localhost:4502/content/calix/en/site/home.html |
| **Subject Type** | Username | **Issuer** | https://calix--SFDEV2.cs12.my.salesforce.com |
| **Name ID Format** | urn:oasis:names:tc:SAML:2.0:nameid-format:persistent |  |  |
| **Verify Request Signatures** |  |  |  |

### SAML Login Information

|  |  |
| --- | --- |
| View and download SAML endpoint metadata for your organization, communities, or custom domains. | |
| Your Organization | |
| **IdP-Initiated Login URL** | [https://calix--SFDEV2.cs12.my.salesforce.com/idp/login?app=0spV0000000CaXF](https://calix--sfdev2.cs12.my.salesforce.com/idp/login?app=0spV0000000CaXF) |
| **SP-Initiated POST Endpoint** | https://calix--SFDEV2.cs12.my.salesforce.com/idp/endpoint/HttpPost |
| **SP-Initiated Redirect Endpoint** | https://calix--SFDEV2.cs12.my.salesforce.com/idp/endpoint/HttpRedirect |
| **Metadata Discovery Endpoint** | https://calix--SFDEV2.cs12.my.salesforce.com/.well-known/samlidp/Calix\_AEM\_Dev\_Local\_SAML\_POC.xml  https://calix--sfdev2.cs12.my.salesforce.com/s.gif |

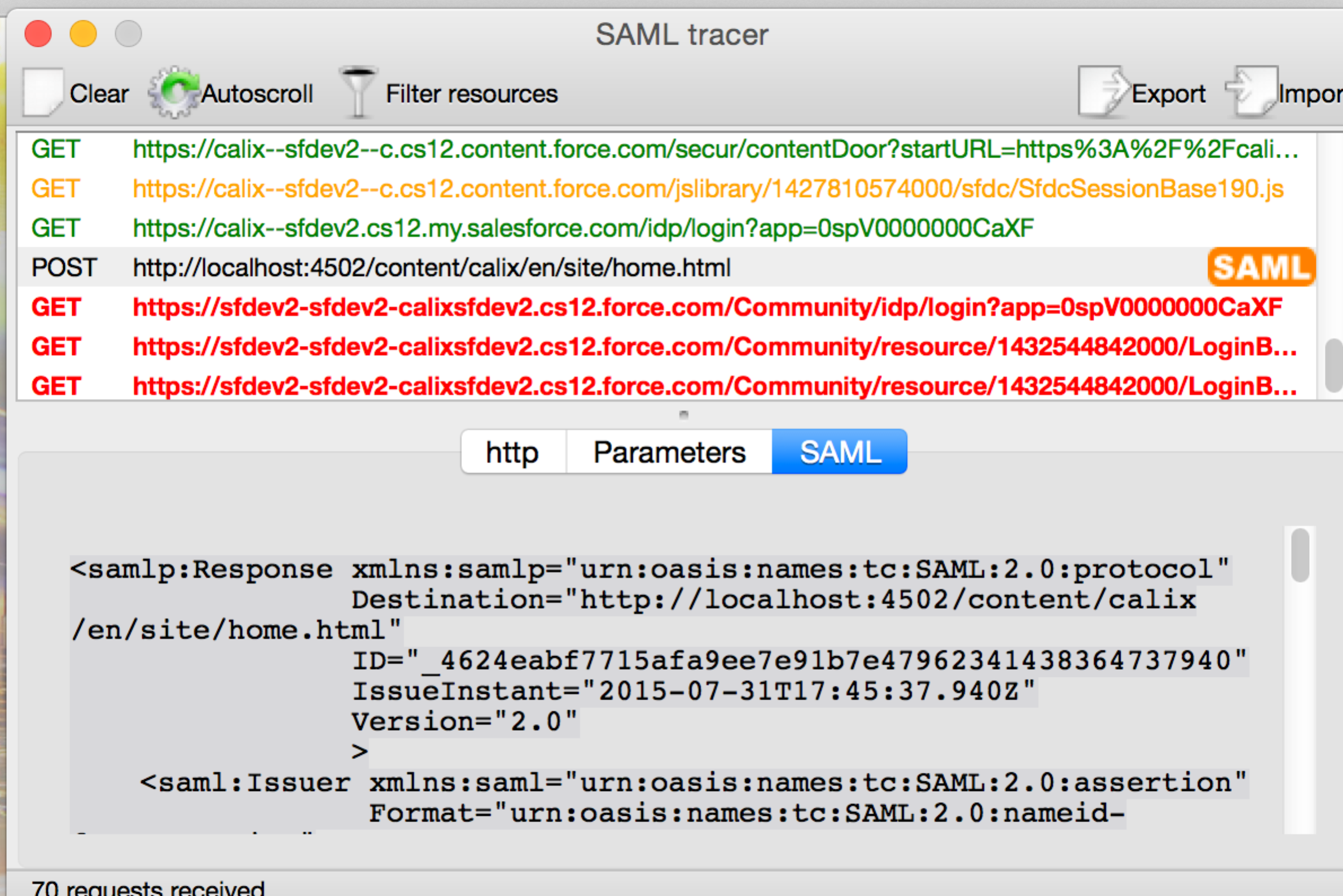
**ide Section - For Communities**

### For Communities

|  |  |
| --- | --- |
| Community Name: Calix Community | |
| **IdP-Initiated Login URL** | <https://sfdev2-sfdev2-calixsfdev2.cs12.force.com/Community/idp/login?app=0spV0000000CaXF> |
| **SP-Initiated POST Endpoint** | https://sfdev2-sfdev2-calixsfdev2.cs12.force.com/Community/idp/endpoint/HttpPost |
| **SP-Initiated Redirect Endpoint** | https://sfdev2-sfdev2-calixsfdev2.cs12.force.com/Community/idp/endpoint/HttpRedirect |
| **Metadata Discovery Endpoint** | https://sfdev2-sfdev2-calixsfdev2.cs12.force.com/Community/.well-known/samlidp/Calix\_AEM\_Dev\_Local\_SAML\_POC.xml  https://calix--sfdev2.cs12.my.salesforce.com/s.gif |

## SAML response posted to AEM from SF

|  |
| --- |
| <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"                  Destination="http://localhost:4502/content/calix/en/site/home.html"                  ID="\_e109b169b471def70ecbdccb14d888c71438375534513"                  IssueInstant="2015-07-31T20:45:34.513Z"                  Version="2.0"                  >      <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"                   Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"                   >https://calix--SFDEV2.cs12.my.salesforce.com</saml:Issuer>      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">          <ds:SignedInfo>              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />              <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />              <ds:Reference URI="#\_e109b169b471def70ecbdccb14d888c71438375534513">                  <ds:Transforms>                      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />                      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">                          <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"                                                  PrefixList="ds saml samlp xs xsi"                                                  />                      </ds:Transform>                  </ds:Transforms>                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />                  <ds:DigestValue>1mF+Cv/1aEwzmmiZXjli2etjuSw=</ds:DigestValue>              </ds:Reference>          </ds:SignedInfo>          <ds:SignatureValue>  CdGkCBjjvP7I6rbzJ0EYywiD3/Qong/8f19xSKD24aEgOG8RZEDxCSG7QrssvJ80JChLwj+CU79M  ZdWLC3cXBYI2e0Vo+RbvAbHe8C6EAYs+GOrEmmF/af12B4uodNqozCu1V6WjVKXACAX8EWcQzseJ  om7o8vDskC4c+ZPqWWiQ+Nc+lUW3cl0h6sOVWBbuE/ZBNuvkteFQYHhPE1UGzRSpzYFUBEzNyhgL  rOBSc0/0dHSpRRFtSUKJOl1z6qeM9RSoRl940+Ri0Vxmttgf8lXvMjxd1EqGO3mLqygeZkx8HXWg  zg9VUISrj89iJLiMGMPwhtH9NXYiNn5q1hFnwQ==  </ds:SignatureValue>          <ds:KeyInfo>              <ds:X509Data>                  <ds:X509Certificate>MIIErDCCA5SgAwIBAgIOAUobotEjAAAAABtAzGcwDQYJKoZIhvcNAQEFBQAwgZAxKDAmBgNVBAMM  H1NlbGZTaWduZWRDZXJ0XzA1RGVjMjAxNF8xODA3NDExGDAWBgNVBAsMDzAwRFYwMDAwMDA4OFBI  YzEXMBUGA1UECgwOU2FsZXNmb3JjZS5jb20xFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xCzAJBgNV  BAgMAkNBMQwwCgYDVQQGEwNVU0EwHhcNMTQxMjA1MTgwNzQyWhcNMTYxMjA0MTgwNzQyWjCBkDEo  MCYGA1UEAwwfU2VsZlNpZ25lZENlcnRfMDVEZWMyMDE0XzE4MDc0MTEYMBYGA1UECwwPMDBEVjAw  MDAwMDg4UEhjMRcwFQYDVQQKDA5TYWxlc2ZvcmNlLmNvbTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNj  bzELMAkGA1UECAwCQ0ExDDAKBgNVBAYTA1VTQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC  ggEBAK0en1KeuTjYR7ljLKhcR3sHBHofLiST1bK0ygC2OM4UMbHePKBlV9ZdaeaPM7dXoi/0UyJX  knX5CoJQxPO8NVmSR1HQj7paXLMf2y7774M2JvXyw+LGdRG3aZialqG4gdBJc1Lw2YWldDSFYoKo  RkahX18CIF99MtRJnCxjICR0eMu+wSG1g4EFU4cPCmAr0+bNtEM3hozVDpPaghLnnFE7h1Svbdx+  ugEHFlrRwa2yS76K7JEL8tuwQ6g+ag2dQadRKkdRv4LFyESVU6E5u1BEuNEIXszj7XV1Yq3B6un0  oxO1e6PREdRYR5MSDm6dyW80CKf+sAkwNj+nefPB4Y0CAwEAAaOCAQAwgf0wHQYDVR0OBBYEFAVt  hmiV/P9drc+gbVC8xJ4R8m6BMIHKBgNVHSMEgcIwgb+AFAVthmiV/P9drc+gbVC8xJ4R8m6BoYGW  pIGTMIGQMSgwJgYDVQQDDB9TZWxmU2lnbmVkQ2VydF8wNURlYzIwMTRfMTgwNzQxMRgwFgYDVQQL  DA8wMERWMDAwMDAwODhQSGMxFzAVBgNVBAoMDlNhbGVzZm9yY2UuY29tMRYwFAYDVQQHDA1TYW4g  RnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNBgg4BShui0TsAAAAAG0DMZzAPBgNV  HRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBQsDpYsrhrPohj9J0xH9jhSualJXCQLwBy  o30YeQ4W/7gxtV0tDk3C4UNx8KF7EFJYwjlgbmaf8wDH6obuBdl7p3HUfSGzA68tX4GQUuKg+38Y  2UjEoXRNY+FmfuYBDmbpwgWbX0tmTOu5adzrbdFjmdUuaXx2YP18kCKU0D3v8dZUwBWUq5h3VZMy  RoSwCb/qSJUX60eJzL6A8dai5ulGl1zEmoPsVMcD7O7h8iGnr+SUuaBq46MnnLBRR67WUGKgmIOI  4kT413vNpL0iBR2cOHyIlVOir0iVgaUW0tI6FIMT54B27KOdeyXnXPfzgdyFKEDAFQvegXG+boQc  Z/ya</ds:X509Certificate>              </ds:X509Data>          </ds:KeyInfo>      </ds:Signature>      <samlp:Status>          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />      </samlp:Status>      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"                      ID="\_69a394b35078bd9bba6c003d3a5a95d51438375534513"                      IssueInstant="2015-07-31T20:45:34.513Z"                      Version="2.0"                      >          <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"                       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"                       >https://calix--SFDEV2.cs12.my.salesforce.com</saml:Issuer>          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">              <ds:SignedInfo>                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />                  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />                  <ds:Reference URI="#\_69a394b35078bd9bba6c003d3a5a95d51438375534513">                      <ds:Transforms>                          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />                          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">                              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"                                                      PrefixList="ds saml xs"                                                      />                          </ds:Transform>                      </ds:Transforms>                      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />                      <ds:DigestValue>Ilu7npjPstiiJm7yStBZovj7W0I=</ds:DigestValue>                  </ds:Reference>              </ds:SignedInfo>              <ds:SignatureValue>  MC9BpthXDnqu6r7vJBzE+G43m4MRQIR6PF6uKTyMe32ZY1qIZWuvep9qCh3IYNKeIqgw4uLir+7Z  AmAJmtKB7FWMpfS177WTDINGSSOa1N0PCUA64BtZ8DdwH6SE0SilzomEGUpBZxchsXA8rNukOyy0  r7hEOtqTnT/UHK5V7kN7L/kvx26ppNaDGDlfba0Ufg+ZY+WPvhLXkaRm+Mjlnj4xeypFUNoL1vak  5u0ut+6i5kJkdzTFu+DjQvEGZM7xnkQPzI1bzYMVXMcnFOI8FhhSH+5x/5tfAoKmFXHfqO3njnit  cGaC6RF9Md/2/V+dWCEzxnEnnymhXr2MD4hEWw==  </ds:SignatureValue>              <ds:KeyInfo>                  <ds:X509Data>                      <ds:X509Certificate>MIIErDCCA5SgAwIBAgIOAUobotEjAAAAABtAzGcwDQYJKoZIhvcNAQEFBQAwgZAxKDAmBgNVBAMM  H1NlbGZTaWduZWRDZXJ0XzA1RGVjMjAxNF8xODA3NDExGDAWBgNVBAsMDzAwRFYwMDAwMDA4OFBI  YzEXMBUGA1UECgwOU2FsZXNmb3JjZS5jb20xFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xCzAJBgNV  BAgMAkNBMQwwCgYDVQQGEwNVU0EwHhcNMTQxMjA1MTgwNzQyWhcNMTYxMjA0MTgwNzQyWjCBkDEo  MCYGA1UEAwwfU2VsZlNpZ25lZENlcnRfMDVEZWMyMDE0XzE4MDc0MTEYMBYGA1UECwwPMDBEVjAw  MDAwMDg4UEhjMRcwFQYDVQQKDA5TYWxlc2ZvcmNlLmNvbTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNj  bzELMAkGA1UECAwCQ0ExDDAKBgNVBAYTA1VTQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC  ggEBAK0en1KeuTjYR7ljLKhcR3sHBHofLiST1bK0ygC2OM4UMbHePKBlV9ZdaeaPM7dXoi/0UyJX  knX5CoJQxPO8NVmSR1HQj7paXLMf2y7774M2JvXyw+LGdRG3aZialqG4gdBJc1Lw2YWldDSFYoKo  RkahX18CIF99MtRJnCxjICR0eMu+wSG1g4EFU4cPCmAr0+bNtEM3hozVDpPaghLnnFE7h1Svbdx+  ugEHFlrRwa2yS76K7JEL8tuwQ6g+ag2dQadRKkdRv4LFyESVU6E5u1BEuNEIXszj7XV1Yq3B6un0  oxO1e6PREdRYR5MSDm6dyW80CKf+sAkwNj+nefPB4Y0CAwEAAaOCAQAwgf0wHQYDVR0OBBYEFAVt  hmiV/P9drc+gbVC8xJ4R8m6BMIHKBgNVHSMEgcIwgb+AFAVthmiV/P9drc+gbVC8xJ4R8m6BoYGW  pIGTMIGQMSgwJgYDVQQDDB9TZWxmU2lnbmVkQ2VydF8wNURlYzIwMTRfMTgwNzQxMRgwFgYDVQQL  DA8wMERWMDAwMDAwODhQSGMxFzAVBgNVBAoMDlNhbGVzZm9yY2UuY29tMRYwFAYDVQQHDA1TYW4g  RnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNBgg4BShui0TsAAAAAG0DMZzAPBgNV  HRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBQsDpYsrhrPohj9J0xH9jhSualJXCQLwBy  o30YeQ4W/7gxtV0tDk3C4UNx8KF7EFJYwjlgbmaf8wDH6obuBdl7p3HUfSGzA68tX4GQUuKg+38Y  2UjEoXRNY+FmfuYBDmbpwgWbX0tmTOu5adzrbdFjmdUuaXx2YP18kCKU0D3v8dZUwBWUq5h3VZMy  RoSwCb/qSJUX60eJzL6A8dai5ulGl1zEmoPsVMcD7O7h8iGnr+SUuaBq46MnnLBRR67WUGKgmIOI  4kT413vNpL0iBR2cOHyIlVOir0iVgaUW0tI6FIMT54B27KOdeyXnXPfzgdyFKEDAFQvegXG+boQc  Z/ya</ds:X509Certificate>                  </ds:X509Data>              </ds:KeyInfo>          </ds:Signature>          <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">              <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">salesforcesystem@calix.com.sfdev2</saml:NameID>              <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">                  <saml:SubjectConfirmationData NotOnOrAfter="2015-07-31T20:50:34.513Z"                                                Recipient="http://localhost:4502/content/calix/en/site/home.html"                                                />              </saml:SubjectConfirmation>          </saml:Subject>          <saml:Conditions NotBefore="2015-07-31T20:45:04.513Z"                           NotOnOrAfter="2015-07-31T20:50:34.513Z"                           xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"                           >              <saml:AudienceRestriction>                  <saml:Audience>calix-dev-localhost-poc</saml:Audience>              </saml:AudienceRestriction>          </saml:Conditions>          <saml:AuthnStatement AuthnInstant="2015-07-31T20:45:34.513Z"                               xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"                               >              <saml:AuthnContext>                  <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>              </saml:AuthnContext>          </saml:AuthnStatement>          <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">              <saml:Attribute Name="userId"                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"                              >                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"                                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"                                       xsi:type="xs:anyType"                                       >00570000001mmT7</saml:AttributeValue>              </saml:Attribute>              <saml:Attribute Name="username"                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"                              >                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"                                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"                                       xsi:type="xs:anyType"                                       >salesforcesystem@calix.com.sfdev2</saml:AttributeValue>              </saml:Attribute>              <saml:Attribute Name="email"                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"                              >                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"                                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"                                       xsi:type="xs:anyType"                                       >muralikrishna.sara@calix.com</saml:AttributeValue>              </saml:Attribute>              <saml:Attribute Name="is\_portal\_user"                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"                              >                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"                                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"                                       xsi:type="xs:anyType"                                       >false</saml:AttributeValue>              </saml:Attribute>          </saml:AttributeStatement>      </saml:Assertion>  </samlp:Response> |



## Overall result

**The flow keeps going in loop as follows:**

User request /content/calix/\*\* page -> AEM redirects to SF community login page -> User logs in successfully -> SF POSTs SAML data to AEM page -> AEM does not process this SAML data and considers the user as anonymous -> goes to step 1 again to redirect to SF community login page.

## AEM error.log

31.07.2015 16:02:19.028 \*INFO\* [qtp471945900-11926] org.apache.sling.auth.core.impl.SlingAuthenticator getAnonymousResolver: Anonymous access not allowed by configuration - requesting credentials

31.07.2015 16:02:51.070 \*INFO\* [qtp471945900-11743] org.apache.sling.auth.core.impl.SlingAuthenticator getAnonymousResolver: Anonymous access not allowed by configuration - requesting credentials