SETUP GUIDE JBOSS KEYCLOAK AS IdP

STEP 1:

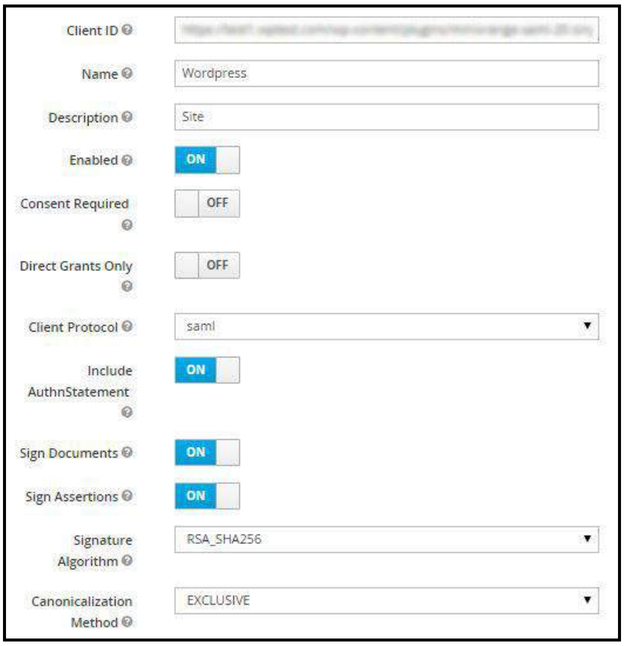
- In your Keycloak admin console, select the realm that you want to use.
- From left menu, select **Clients**.
- Create a new client/application.
- Configure the following:

Client ID	The **SP-EntityID / Issuer** from the step 1 of the plugin under Identity Provider tab.
Name	Provide a name for this client (Eg. Wordpress)
Description	Provide a description (Eg. wordpress site)
Enabled	ON
Client Protocol	SAML
Include AuthnStatement	ON
Sign Documents	ON
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Canonicalization Method	EXCLUSIVE
Force Name ID Format	ON
Name ID Format	Email
Root URL	The **ACS (AssertionConsumerService) URL** from the step 1 of the plugin under Identity Provider tab.
Valid Redirect URIs	The **ACS (AssertionConsumerService) URL** from the step 1 of the plugin under Identity Provider tab.

- Under **Fine Grain SAML Endpoint Configuration**, configure the following:

Assertion Consumer Service POST Binding URL	The **ACS (AssertionConsumerService) URL** from the step 1 of the plugin under Identity Provider tab.
Logout Service Redirect Binding URL	The **Single Logout URL** from the step 1 of the plugin under Identity Provider tab.

- Click on **Save**.

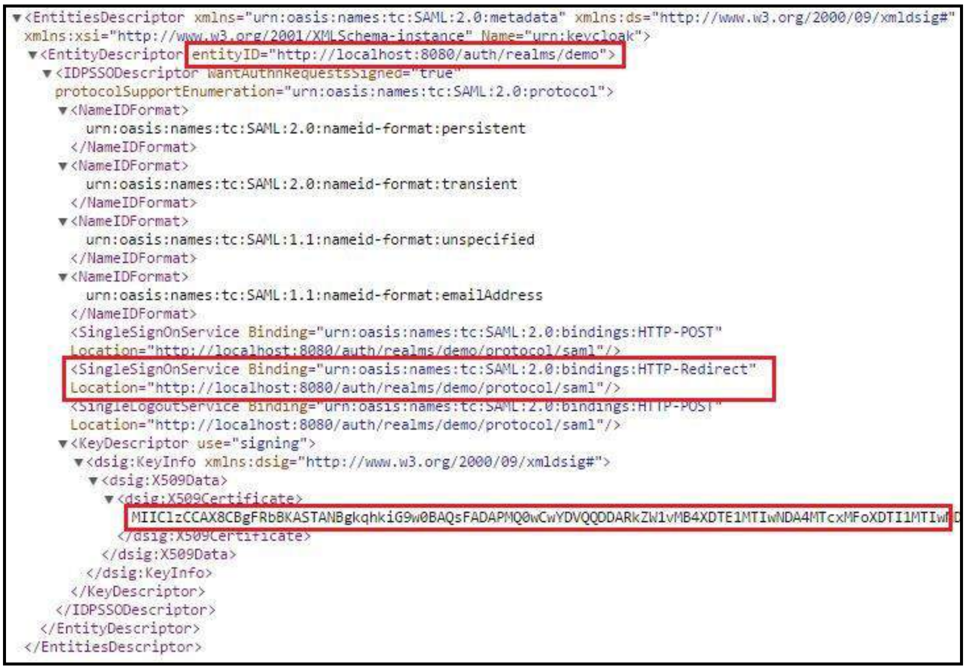


Client ID	[redacted]
Name	Wordpress
Description	Site
Enabled	ON
Consent Required	OFF
Direct Grants Only	OFF
Client Protocol	saml
Include AuthnStatement	ON
Sign Documents	ON
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Canonicalization Method	EXCLUSIVE

STEP 2:

- Go to, **http://<YOUR_DOMAIN>/auth/realms/{YOUR_REALM}/protocol/saml/descriptor**. This will open an XML in the browser.
- Go to **Service provider** Tab in **miniOrange SAML Plugin** and enter the following details:

Identity Provider Name	Keycloak
SAML Login URL	Search for `SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"` Enter the Location value in the textbox.
IdP Entity ID or Issuer	Search for *`entityID`*. Enter it's value in this textbox.
X.509 Certificate*	Enter the *`X509Certificate`* tag value in this textbox.
Response Signed	Checked
Assertion Signed	Checked



```
▼<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Name="urn:keycloak">
  ▼<EntityDescriptor entityID="http://localhost:8080/auth/realms/demo">
    ▼<IDPSSODescriptor WantAuthnRequestsSigned="true"
     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      ▼<NameIDFormat>
         urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
       </NameIDFormat>
      ▼<NameIDFormat>
         urn:oasis:names:tc:SAML:2.0:nameid-format:transient
       </NameIDFormat>
      ▼<NameIDFormat>
         urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
       </NameIDFormat>
      ▼<NameIDFormat>
         urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
       </NameIDFormat>
       <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
       Location="http://localhost:8080/auth/realms/demo/protocol/saml"/>
       <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
       Location="http://localhost:8080/auth/realms/demo/protocol/saml"/>
       <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
       Location="http://localhost:8080/auth/realms/demo/protocol/saml"/>
      ▼<KeyDescriptor use="signing">
        ▼<dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
          ▼<dsig:X509Data>
            ▼<dsig:X509Certificate>
               MIIClzCCAX8CBgFRbBKASTANBgkqhkiG9w0BAQsFADAPMQ0wCwYDVQQDDARkZW1vMB4XDTE1MTIwNDA4MTcxMFoXDTI1MTIwM
             </dsig:X509Certificate>
           </dsig:X509Data>
         </dsig:KeyInfo>
       </KeyDescriptor>
     </IDPSSODescriptor>
   </EntityDescriptor>
 </EntitiesDescriptor>
```