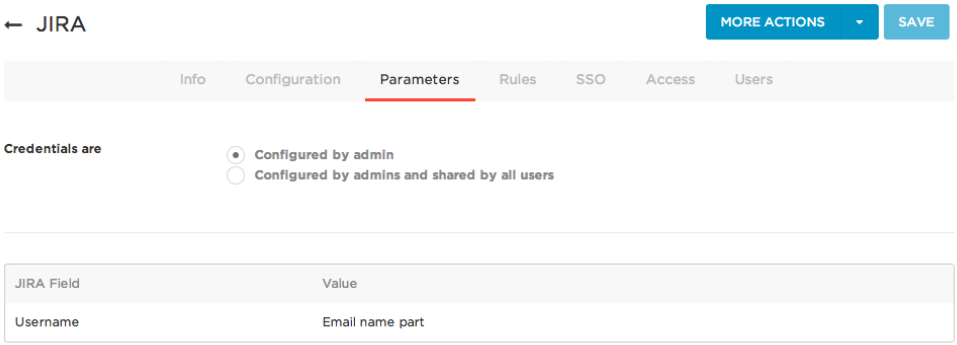
# Configuring SAML for Atlassian JIRA version 6 on Linux

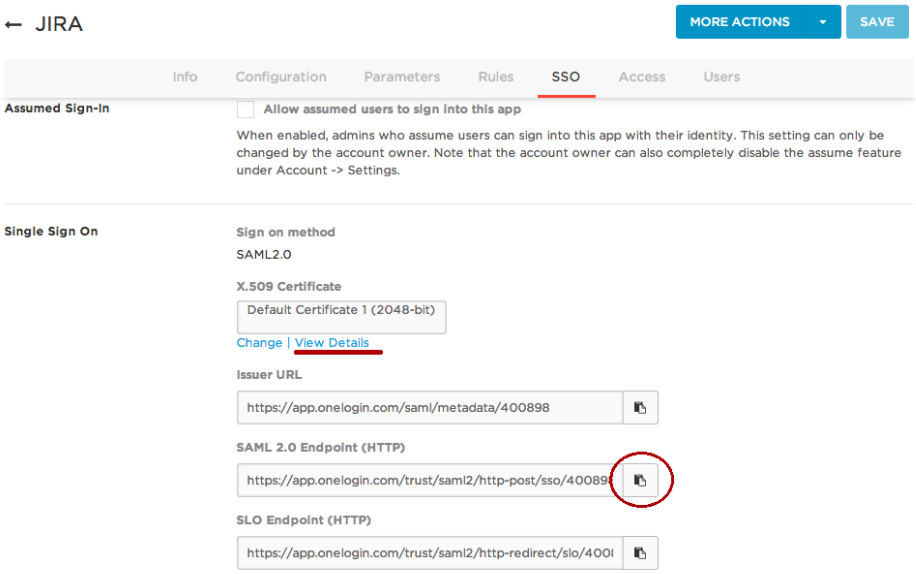
## OneLogin Configuration

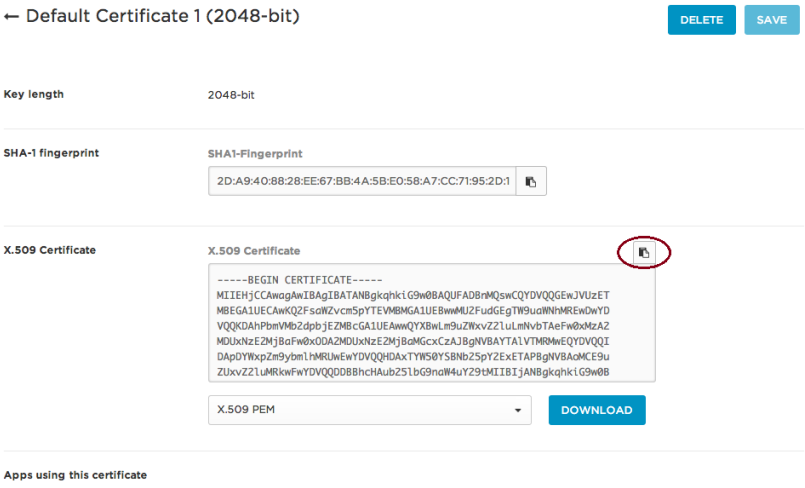
1. Go to **Apps > Find Apps**. Search for "JIRA" and add JIRA
2. In the subsequent page select SAML 2.0 for the Connector Version and click **Continue**.
3. Select Configuration and insert the Login URL value. If you access JIRA at http://jiraserver:8080 - you would add jiraserver:8080 to this field


4. Click the **Parameters** tab and select **Configured by admin**. Generally, you want to use Email name part for **Username**.




5. Click the **SSO** tab and copy with the button **SAML Login URL** and click on **View Details** to see the certificate:






6. Under **Access** and **Users**, assign the JIRA app to the appropriate Role in OneLogin and independent users.
7. Select **save**, you are now done.

## JIRA Configuration

1. Edit the jira_onelogin.xml to include your x509 certificate from OneLogin and the SAML Login URL we made note of in step 4 above.
2. Open jira_onelogin.xml in a text editor and copy the value of the x509 certificate from your OneLogin account between the <certificate></certificate> tags - remove all line feeds/carriage returns in the certificate value.

```
<config><certificate>MIICMTCCAiWgAwIBAgIBATADBgEAMGcxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRUwEw
YDVQQHDAMA8GA1UECgwIT25lTG9naW4xGTAXBgNVBAMMEGFwcC5vbmVsb2dpbi5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggE
KAoIBAQDKvNTqqXMUv2kbVIaAeov5qOaVrbDQwj/65aaCs8CuXwC1Ks69Z3/D5qGHLDqVCR7+BhbVEiZRK/tb/LcW1qsFySXlgbGY5z
qvHXjQ2ChYDofpTV8iMr7klHBXweP+pxvrknsmMUxlmaH7gcvRBN9UkdXds0pXTYBho0TnCDljEvktwKg7e02FyUgwM1xSJSYTm3IDV
NSyfWiZ4H51vOUz80ulIUoHtu5WHPdvzP3vdokRbW5akN/rE2T6ws0CuTdd+LKyxdIuuJP3MseMG8HIf9C/4wWXkxWB9amCzujsmBJu
aEduKX0OP7T8XyOZoQ7A0BjMl8eqxx/rOmr6O0ztAgMBAAEwAwYBAAMBAA==</certificate><assertion>http://server1:808
0/login.jsp</assertion><issuer>http://server1:8080/secure/Dashboard.jspa</issuer><ssotarget>https://app
.onelogin.com/saml/signon/49097</ssotarget></config>
```

**Note:** The default JIRA_INSTALL directory is **/opt/atlassian/jira**)

3. Copy the jira_onelogin.xml file into JIRA_INSTALL and JIRA_INSTALL/bin directory.

4. Copy the customauth-jira-6.1.jar file into JIRA_INSTALL/atlassian-jira/WEB-INF/lib directory

5. Open in your text editor the file named **seraph-config.xml** which can be found on the Jira server into JIRA_INSTALL/atlassian-jira/WEB-INF/classes directory

6. From within this file, do the following:

   a. Modify the login.url parameter. Find the line <param-name>link.login.url</param-name> and make sure the corresponding value is

```
<param-name>link.login.url</param-name>
<param-value>/login.jsp?os_destination=${originalurl}</param-value>
```

   b. Comment out the following line:

```
before: <authenticator class="com.atlassian.jira.security.login.JiraSeraphAuthenticator"/>
after: <!--<authenticator class="com.atlassian.jira.security.login.JiraSeraphAuthenticator"/>-->
```

   c. Add the following before the <services> tag

```
<authenticator class="com.onelogin.jira.saml.SSOAuthenticator"/>
```

d. Save and close the seraph-config.xml file

7. Open in your text editor the file named loginform.jsp located in JIRA_INSTALL/atlassian-jira/includes directory

8. From within this file, do the following:

a. Find the line: <%@ page import="com.atlassian.jira.web.filters.JiraLoginInterceptor" %> and add the following on the line below it:

```
<%@ page import= "com.onelogin.jira.saml.SSOAuthenticator" %>
```

b. Within loginform.jsp locate the following line:

```
request.setAttribute("loggedInUser", jiraAuthenticationContext.getLoggedInUser()
== null ? null : jiraAuthenticationContext.getLoggedInUser().getDisplayName());
```

c. Add the following immediately after:

```
if(request.getParameter("SAMLResponse") == null)
    {
        String redirectURL = request.getSession().getAttribute("reqString").toString();
        response.sendRedirect(redirectURL);
    }else{

        if(jiraAuthenticationContext.getLoggedInUser() != null)
        {

            if(request.getSession().getAttribute("os_destination") != null)
            {
                String os_destination =
                          request.getSession().getAttribute("os_destination").toString();
                response.sendRedirect(os_destination);
            }else{
                response.sendRedirect("/");
            }
        }
    }
```

d. Save and close the loginform.jsp file

9. Restart the Atlassian JIRA service on the server.