Configuring ClearQuest for SAML2 SSO

Security Assertion Markup Language (SAML) 2.0 is a standard for exchanging authentication and authorization data between security domains. ClearQuest® can be configured to use SAML2 Identity providers (IDPs) for single sign-on (SSO).

When ClearQuest is configured to use SAML2 for SSO, then when an unauthenticated user connects to CQ Web, they are redirected to the SAML2 IDP for login. Once they successfully login to the IDP, they are redirected to ClearQuest. If there is only one dbset and database, then ClearQuest login proceeds automatically. If there are additional dbsets or databases, then the user is presented with a dialog to choose which database to connect to.

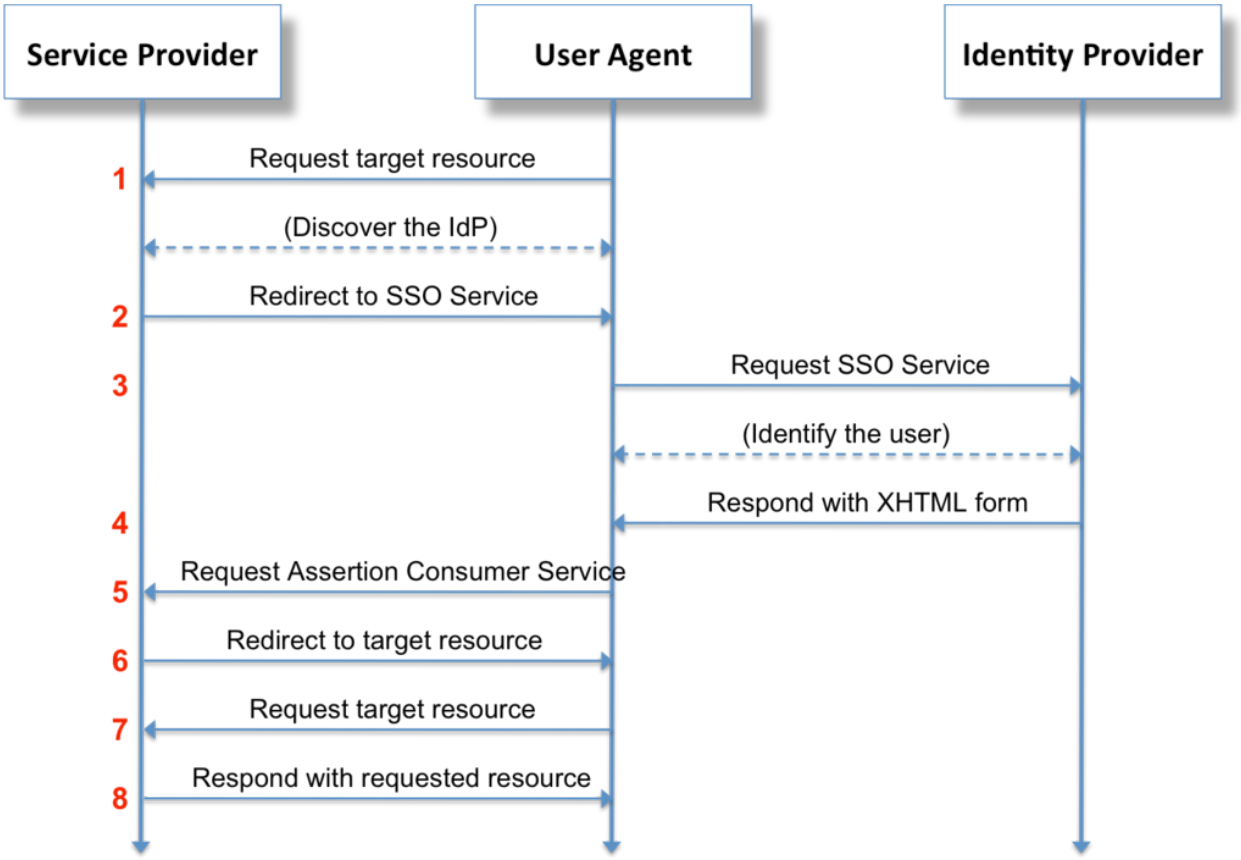


Figure 1 SAML 2.0 Web Browser SSO (SP Redirect Bind/ IdP POST Response) by Tom Scavo
https://creativecommons.org/licenses/by-sa/3.0/

The SAML2 assertions are stored in cookies, along with LTPA2 cookies. If you close your browser and reopen it, you will still be logged in to your SSO provider, but your CQ Web session will have been logged off.

Configuring ClearQuest to use SAML2 for SSO is a three-step process. The first step is to configure the WebSphere profile as a SAML2 Service Provider (SP). The second step is to configure trust with a SAML2 identity provider (IDP). The third step is to configure ClearQuest Web and the ClearQuest database and to use SAML2 for SSO.

Setting up WebSphere Profile as a SAML2 Service Provider

IBM® WebSphere® documentation describes how to configure a WebSphere profile as a SAML2 service provider. General information about SAML2 support can be found in the following help topic: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/cwbs_samlssoconcepts.html

Here are the steps:

Install the SAML ACS application and configure the SAML TAI in the WebSphere profile. See the procedure to enable your system to use the SAML web single sign-on (SSO) feature: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

For **Custom Properties**, you can use the information provided in the following illustration as a guide:

Custom properties

New | Edit | Delete

Select	Name	Value
☐	sso_1.sp.acsUrl	https://adamsweb:9445/samlsps/acs
☐	sso_1.sp.login.error.page	https://https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://adamsweb:9445/samlsps/acs&NameIdFormat=Email&Target=https://adamsweb:9445/cqweb
☐	sso_1.sp.idMap	idAssertion

Apply | OK | Reset | Cancel

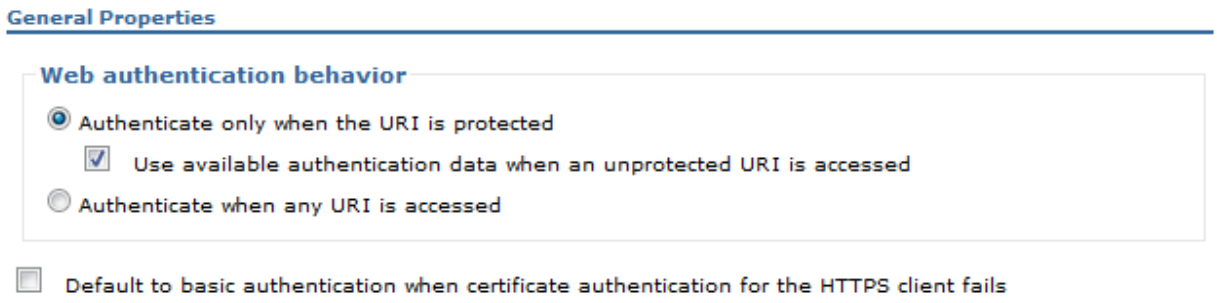
Select	Name	Value
☐	sso_1.sp.login.error.page	https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://ADAMSWEB.dev.ratlcore.ibm.com:9450/samlsps/acs&NameIdFormat=Email&Target=https://ADAMSWEB.dev.ratlcore.ibm.com:9450/cqweb
☐	sso_1.sp.acsUrl	https://ADAMSWEB.dev.ratlcore.ibm.com:9450/samlsps/acs
☐	sso_1.sp.idMap	idAssertion
☐	sso_1.idp_1.EntityID	https://www.myidp.ibm.com/isam/sps/saml20idp/saml20
☐	sso_1.idp_1.SingleSignOnUrl	https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/login
☐	sso_1.sp.targetUrl	https://ADAMSWEB.dev.ratlcore.ibm.com:9450/cqweb
☐	sso_1.sp.trustAnySigner	true
☐	sso_1.sp.wantAssertionsSigned	false
☐	sso_1.idp_1.certAlias	vmssoidp
☐	sso_1.sp.trustedAlias	vmssoidp

For more information about custom properties, see the following help topic:
http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

Note: You can also use the AdminTask.addSAMLTAISSO command to add the SAML TAI and set its custom properties, see the following help topic:
http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_addsamltaisso.html

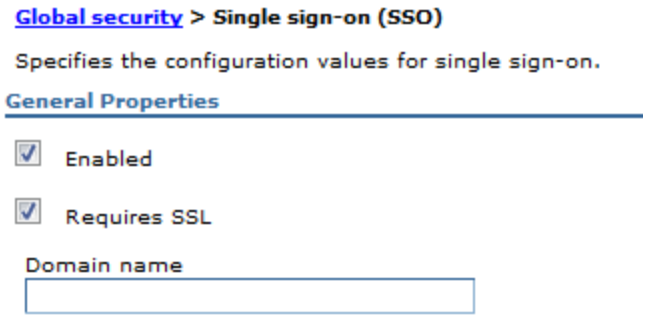
Ensure that SSO is enabled in WebSphere Global Security. These boxes must be checked in **Security > Global security**

For **Security > Global security > Authentication > Web and SIP Settings > General Settings >**



This ensures that SSO is triggered if any CQ Web resource is requested.

Single sign-on (SSO) >

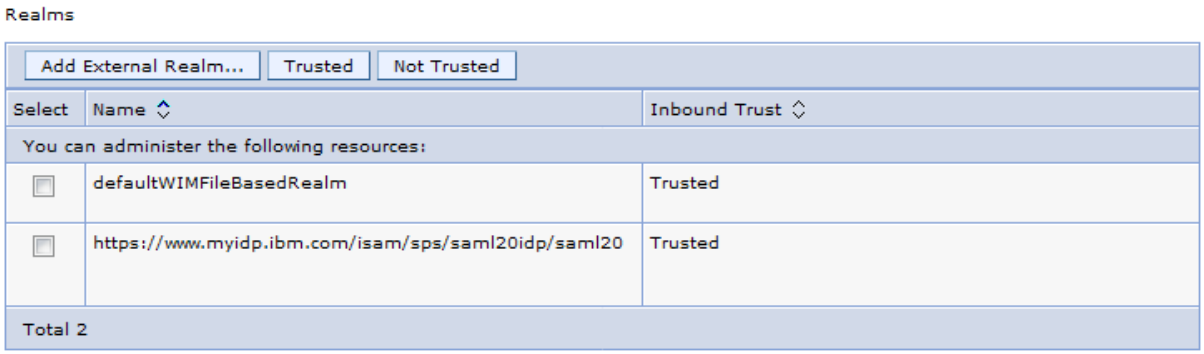


If necessary, add a Domain name to trust. This would be the minimum part of the domain that matches your identity provider, for example, ".ibm.com".

While you are here, ensure that the SAML Identity Providers realm is trusted. Go to **Security > Global security**. In **user account repository**, click **Configure**. Click **Trusted authentication realms – inbound**. Click **Add External Realm** and fill in the external realm name. Click **OK** and save your changes to the mastedr configuration.

Alternative steps, including wsadmin scripts, can be found in part two of the following help topic: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_configuresamlssopartners.html

For example, the following shows WebSphere trusting the realm from an IBM ISAM Identity Provider with the realm https://www.myidp.ibm.com/isam/sps/saml20idp/saml20.


Realms

Add External Realm... | Trusted | Not Trusted

Select	Name	Inbound Trust
You can administer the following resources:		
☐	defaultWIMFileBasedRealm	Trusted
☐	https://www.myidp.ibm.com/isam/sps/saml20idp/saml20	Trusted
Total 2		

Configure Trust with an Identity Provider

The WebSphere profile (the service provider) you configured above must be told that it can trust the identity provider (SiteMinder, ISAM, and so forth). As well, the identity provider must be told it can trust the WebSphere service provider that is hosting ClearQuest Web. Follow the steps below for establishing this trust.

Note: Consult an expert in the identity provider software that you use for help determining what values to use in the commands described in the links below.

Tell the Identity Provider to Trust the Service Provider (CQ Web)

1) Follow the steps below to export a metadata file for the service provider (WebSphere profile hosting CQ Web). Run these commands for the same WebSphere profile you have CQ Web installed in. See the procedure in the following help topic: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_exportsamlspmetadata.html

2) Import this metadata file into your identity provider. This needs to be done by the administrator of your SAML2 Identity Provider.

Tell the Service Provider to Trust the Identity Provider

1) Export your SAML2 Identity Provider's metadata to a file. This needs to be done by the administrator of your SAML2 Identity Provider.
2) Import the SAML2 Identity Provider's metadata into the Service Provider (WebSphere profile hosting CQ Web). See the procedure in the following help topic: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_importsamlidpmetadata.html

ClearQuest SSO Setup

ClearQuest configuration for SSO follows almost the same directions as in the help topic Configuring strong authentication with smart-cards.

The steps to set up SSO with SAML2 are

1) Configure ClearQuest database for SSO
2) Configure ClearQuest Web server for SSO
3) Map LTPA/LDAP users to CQ Web application

Configure ClearQuest database for SSO

1) You must set an SSO password in the database. See the procedure in help topic Configuring ClearQuest databases for container authentication.
2) Create an sso.properties file using cqrpc/cqrpc.exe and the password you used in step 1. See the procedure in help topic Configuring ClearQuest Web server for container authentication.
   Note: The sso.properties generated by cqrpc should remain in the same directory as the cqrpc executable. This file is used by the cqrpc executable as well. This sso.properties file is different than the one you edit in step 3, below.
   Configure the sso.properties file for SAML2. See the procedure in help topic Configuring the ClearQuest Web client for container authentication.
   For the SAML2, in sso.properties, the SSO_LOGIN_MODE should be set to "SAML2".

Configure ClearQuest Web server for SSO

Reference the help topic Configuring client certificate authentication for ClearQuest Web to modify the web.xml descriptor, but for the security constraint and other clauses in web.xml use this:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>secure</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>ClearQuestUsers</role-name>
    </auth-constraint>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>CQBridge</web-resource-name>
        <!-- <url-pattern>/oslc/*</url-pattern> -->
        <url-pattern>/oslc/repo/sso2/discovery</url-pattern>
        <url-pattern>/oauth-request-consumer/*</url-pattern>
        <url-pattern>/oauth-authorize-consumers/*</url-pattern>
        <url-pattern>/oauth-request-token/*</url-pattern>
        <url-pattern>/oauth-authorization/*</url-pattern>
        <url-pattern>/oauth-access-token/*</url-pattern>
        <url-pattern>/scripts/*</url-pattern>
        <url-pattern>/images/*</url-pattern>
        <url-pattern>/stylesheets/*</url-pattern>
        <url-pattern>/gadgets/*</url-pattern>
        <url-pattern>/cqquerywizard.cq</url-pattern>
        <url-pattern>/cqartifactdetails.cq</url-pattern>
        <url-pattern>/cqqueryresults.cq</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
</security-constraint>

<security-role>
    <role-name>ClearQuestUsers</role-name>
</security-role>
```

Map authenticated users to CQ Web application

Currently there is no way to choose which SAML2 authenticated users can access the ClearQuest Web application. You must allow all authenticated users access to the application. Just accessing the application, however, does not mean that they can actually log in to ClearQuest Web, it only means that they can load the CQ Web resources in their browser. Whether they can actually log in to a ClearQuest database depends on whether the user is already subscribed to the ClearQuest database. For example, if the user "tom" is allowed access to the CQ Web application but does not have any access to a ClearQuest database, they will only see the database selection dialog but will not be able to actually connect to the database.

To map SAML2 authenticated users to the CQ Web application, follow these steps:

1) Using the WebSphere Application Server administrative console, click **Applications > Application types > WebSphere enterprise applications** in the navigation pane. The Enterprise Applications page opens.
2) In the Enterprise Applications table, click **TeamEar**. The Configuration page opens.
3) In the **Detail Properties** section, click **Security role to user/group mapping**.
4) In the table row in which the ClearQuestUsers role displays, select the check box in the Select column and click on **Map Special Subjects** and choose **All Authenticated in Trusted Realms**
5) Click **OK** on the Security role to user/group mapping page to save the mappings.
6) Restart the WebSphere Application Server.