# APAR JR63925 Configuring SAML in IBM Business Automation Workflow

## Notes

This guide is to configure SAML in IBM Business Automation Workflow 19.0.0.3 and later.

See [1] for more details and additional configuration options.

## Prerequisites

IBM Business Automation Workflow is connected to the LDAP as Federated Repository.

## Install the SAML ACS application

You can install the SAML ACS application by using the WebSphere Application Server administrative console or by using the python script. The following steps install the SAML ACS application by using the WebSphere Application Server administrative console. For the other option see Reference [2].

1. Install the SAML ACS application using the WebSphere Application Server administrative console:
   1. Login to the WebSphere Application Server administrative console
   2. Navigate to Applications -> New applications
   3. Install the [app\_server\_root](https://help.hcltechsw.com/connections/v55/admin/plan/i_ovr_r_directory_conventions.html#i_ovr_r_directory_conventions__app)/installableApps/WebSphereSamlSP.ear file to your application server

Enable SAML TAI

You can enable SAML TAI be using either the wsadmin command utility or the WebSphere Application Server administrative console. The following steps enable SAML TAI by using or the WebSphere Application Server administrative console. For the other option see Reference [2].

1. Log on to the WebSphere Application Server administrative console.
2. Navigate to Security -> Global security
3. Expand **Web and SIP security** and click **Trust association**
4. Under **General Properties** ensure that the **Enable trust association** option is checked
5. Under Additional Properties select **Interceptors**
6. Click to create a New interceptor
7. Enter com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor in the **Interceptor class name** field.
8. Under **Custom properties**, provide the following custom property information:

|  |  |  |
| --- | --- | --- |
| Property name | Property value | Comment |
| sso\_1.sp.acsUrl | [https://*hostname*:*sslport*/samlsps/<anyURIpatternstring](https://hostname:sslport/samlsps/%3canyURIpatternstring)> | hostname is the host name of the system where WebSphere Application is installed and sslport is the Web server SSL port number |
| sso\_1.sp.idMap, sso\_1.sp.groupMap, sso\_1.sp.groupName | localRealm, idAssertion, | The security context mapping in the service provider is very flexible and configurable.  See details in [3] |

1. Navigate to **Security -> Global security**
2. Click **Custom properties**.
3. Modify or add the following custom properties:

|  |  |
| --- | --- |
| Name | Value |
| com.ibm.websphere.security.DeferTAItoSSO | com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor |
| com.ibm.websphere.security.InvokeTAIbeforeSSO | com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor,com.ibm.ws.security.oauth20.tai.OAuthTAI |

1. Apply and Save the changes.
2. Restart the WebSphere Application Server.

Results: The SAML TAI is now enabled for WebSphere Application Server.

# Configure Single Sign-On Partners

To establish partnerships between the WebSphere Application Server SAML service provider and external SAML identity provider, the identity provider needs to be added using metadata of the identity provider and the SAML token signer certificate needs to be added.  
  
These steps import the IdP metadata using the wsadmin command-line utility and import the SAML token signer certificate using the WebSphere Application Server administrative console. For more options see [3].

1. Add an identity provider to the WebSphere Application Server SAML service provider for single sign-on.  
     
   Prerequisite: From SAML IdP download

* The metadata file in xml format.
* The SAML token signer certificate in pem format.

**Import the IdP metadata file into WebSphere Application Server**

* 1. Start the WebSphere Application Server
  2. start the wsadmin command-line utility import from the app\_server\_root/bin directory by entering the command:  
       
     wsadmin.bat -lang jython -username <bpmadmin> -password <password>
  3. At the wsadmin prompt, enter the following command:   
       
     wsadmin>AdminTask.importSAMLIdpMetadata('-idpMetadataFileName C:\path-to-file\ <IdPMetaDataFile> -idpId 1 -ssoId 1 -signingCertAlias <idpAlias>')
  4. Save the configuration and quit the wsadmin command utility  
       
     wsadmin>AdminConfig.save()  
     wsadmin>quit

**Import the IdP SAML token signer certificate into WebSphere Application Server using the administrative console.**

* 1. Login to the WebSphere Application Server administrative console
  2. Navigate to **Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates**.
  3. Click Add to add the certificate information. Provide the pem file that you downloaded previously.
  4. Specify an alias for the signer certificate
  5. Click **OK** and **Save changes to the master configuration**.
  6. Restart the WebSphere Application Server.

1. Add IdP realms to the list of inbound trusted realms using the administrative console
   1. Click **Global security**.
   2. Under user account repository, click **Configure**.
   3. Click **Trusted authentication realms - inbound**.
   4. Click **Add External Realm**.
   5. Fill in the external realm name.
   6. Click **OK** and **Save changes to the master configuration**.
   7. Restart the WebSphere Application Server.

1. Create SP metadata file and import it into the IdP.
   1. Export the service provider metadata from WebSphere Application Server using the wsadmin command-line utitlity:

wsadmin>**AdminTask.exportSAMLSpMetadata('-spMetadataFileName C:/spdata.xml -ssoId 1')**

* 1. Import the file C:/spdata.xml to the IdP server

1. Ensure IdP configuration has been added to the TAI configuration and add additional security configuration
   1. Navigate to Global security.
   2. Expand Web and SIP security.
   3. Navigate to Trust association > Interceptors > com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor.
   4. Verify that two new properties were added to the SAML TAI configuration: sso\_1.idp\_1.EntityID and sso\_1.idp\_1.SingleSignOnUrl
   5. Add the following properties:

|  |  |  |
| --- | --- | --- |
| Property name | Property value | Comment |
| sso\_1.sp.trustedAlias |  | This value must be the name you gave to the certificate alias when you imported the metadata file. |
| sso\_1.sp.filter | request-url%=/\* | This filter indicates which pages/resources you want to protect IdP SSO |

* 1. Restart the WebSphere Application Server.

Results: Your WebSphere Application Server is now configured as a service provider partner for IdP-initiated SSO.

# References

[1] SAML web single sign-on: <https://www.ibm.com/docs/en/was/8.5.5?topic=au-saml-web-single-sign-1>

[2] Enabling your system to use the SAML web single sign-on (SSO) feature: <https://www.ibm.com/docs/en/was/8.5.5?topic=swss-enabling-your-system-use-saml-web-single-sign-sso-feature-2>

[3] Configuring single sign-on partners: <https://www.ibm.com/docs/en/was/8.5.5?topic=swss-configuring-single-sign-sso-partners-1>