**Cloud Pak for Data on Azure IAM SSO configuration**

**Introduction:**

This document outlines the steps to configure Azure Active directory SAML/SSO configuration for cloud pak for data.

**Documentation Link:**

For better understanding of the SAML authentication in Azure please refer to the below link:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-saml-single-sign-on>

**Pre-requisites:**

1. The azure user id who would be performing this setup should have
   * One of the following roles:
     1. Global Administrator.
     2. Cloud Application Administrator.
     3. Application Administrator.
2. Should have the cloud Pak for data cluster ready.

**Setting up Enterprise Application in Azure AD:**

Please follow the below steps to setup the SAML identity provider (IdP) in AZURE.

1. Login to the Azure portal.
2. From the home page navigate to **Azure Active Directory -> Enterprise Applications -> + New Application > Create your own application**

Graphical user interface, application

Description automatically generated

1. Enter the application name (eg., IBM-CP4D-Support) and click create.
2. Once it is saved, under **Azure Active Directory > Enterprise Applications**, it should show your new application. (eg., IBM-CP4D-Support)

Graphical user interface, text, application, email

Description automatically generated

1. Select the app you just created IBM-CP4D-Support and click on it.
2. Click on 2. Set up single sign on

Graphical user interface, application

Description automatically generated

1. On the Single Sign on page, please select SAML method.

Graphical user interface, application

Description automatically generated

1. In the “Set up Single Sign-on with SAML Page, please input the required values.

Graphical user interface, text, application, email

Description automatically generated

1. In section 1. Basic SAML Configuration, please add the below values for the respective fields.
   1. Identifier (Entity ID) – unique name to identify the application (default ibm\_privatecloud). This entity id will be using the further steps while using samlConfig.json.
   2. Reply URL – https://<cloudpak\_web\_URL>/auth/login/sso/callback
   3. Sign on URL – https://<cloudpak\_web\_URL>
   4. Relay State – optional.
   5. Logout URL - https://<cloudpak\_web\_URL>
2. In section 2. User Attributes and Claims, for Unique User Identifier field change the value as user.mail

Graphical user interface, text, application

Description automatically generated

1. In Section 3. SAML Signing certificate, download the base64 certificate and remove ‘---Begin Certificate ----’ and ‘--- End Certificate ---’ lines and also make sure to convert the multi line file into a single line using any editor and keep it. This will be used while setting up usrmgmt pod in CPD installed names space.

Graphical user interface, application, Word

Description automatically generated

1. Keep the default values in the section 4. The Logon URL will be used as entry point in the samlConfig.json file.

Graphical user interface, text, application, email

Description automatically generated

1. Once the above step is completed, click save and skip the test.
2. Next step is to add the samlConfig.json file in the CP4D usrmgmt pod.

**Setting UP CP4D SSO:**

**Reference link:** <https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/install/saml-sso.html>

Please follow the below steps to configure Single Sign-on for CP4D.

1. Log in to your Red Hat® OpenShift® cluster as a project administrator

*oc login openshift\_url:port*

1. Enable SAML by running the below command.

*oc exec -it -n namespace \*

*$(oc get pod -n namespace -l component=usermgmt | tail -1 | cut -f1 -d\ ) -- bash -c “vi /user-home/\_global\_/config/saml/samlConfig.json”*

Replace the value of namespace where CP4D is installed.

1. In samlconfig.json file, specify the appropriate values for your environment.

{

"entryPoint": "https://login.microsoftonline.com/c1865b6f-1080-45c6-b4e3-7229f279195d/saml2 <the logon URL value from step 4 of the Single Sign on setup > ",

"fieldToAuthenticate": "<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>",

"spCert": "",

"idpCert": "<single line converted certificate base64 file acquired in “Set up Single Sign-on with SAML “ method> ",

"issuer": " Identifier (Entity ID) created in the previous steps.",

"identifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",

"callbackUrl": " <https://cloudpak_web_URL>/auth/login/sso/callback " ,

"disableRequestedAuthnContext": “true”

}

1. Save the file and exit.
2. Run the following command to delete the usermgmt pod.

*oc delete pods -l component=usermgmt*

1. Wait for few minutes for the usermgmt pods to be in running state.
2. After the pods are started please follow the below steps.
   * Go directly to the web client log in page by appending the following path to your Cloud Pak for Data URL: /auth/login/zen-login.html.
   * Log in to the web client as the **admin** user or another administrator with user management permissions.
3. Test the connection from the azure portal.

Graphical user interface, text, application, email

Description automatically generated

1. You should be able to login to CP4D web UI using sso.

A screenshot of a computer

Description automatically generated