**Seas-Okta integration**

**Steps:**

1. Copy the custom jar to seas folder
2. Copy the third-party jars to seas folder
3. Create Authentication definition in SEAS with Okta config
4. Restart Seas
5. Okta settings to enable username instead of mail address
6. Use the Authentication Profile in SSPCM Policy and do the test.

**1.Copy custom jar to seas folder:**

Copy the cignaoktauserexit.jar to the <seas\_install>/lib/custom folder

**2.Copy the third-party jars to seas folder:**

Copy the below jars to <seas\_install>/ lib/thirdparty folder

okta-sdk-api-11.0.2.jar

okta-commons-lang-1.3.4.jar

okta-sdk-impl-11.0.2.jar

okta-http-okhttp-1.3.4.jar

okta-http-api-1.3.4.jar

httpclient5-5.2.1.jar

httpcore5-5.2.2.jar

jackson-databind-2.15.2.jar

jackson-core-2.15.2.jar

snakeyaml-2.0.jar

okta-config-check-1.3.4.jar

jackson-datatype-jsr310-2.15.2.jar

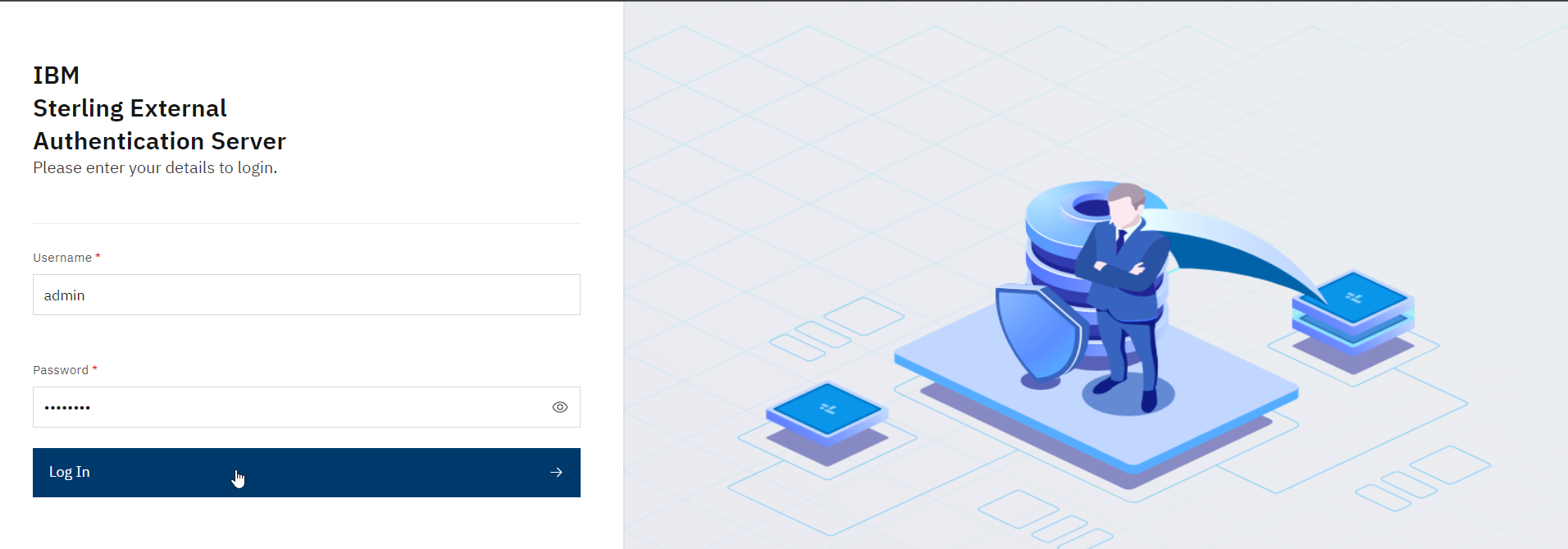
jackson-databind-nullable-0.2.6.jar

jackson-annotations-2.15.2.jar

httpcore5-h2-5.2.2.jar

**3.Create Authentication definition in SEAS with Okta config:**

Login to SEAS UI



Go to Authentication definitions and click on Add Authentication:

A picture containing text, screenshot, software, web page

Description automatically generated

Select Authentication type as Generic, give Name, description and enable Authentication using custom exits

A screenshot of a computer

Description automatically generated

Give class Name as **com.cigna.userexit.oktasso.OktaSsoUserExit** , and add below properties and click save.

OktaApiUrl = dev-82215509.okta.com

OktaApiToken = 00dAbDlxod6dxZgT7W9pbexocEbR7cPl7La8ZaJTVK

UserIdExistsInOkta = true

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Click Next for all other pages(Don’t select anything else) and save the definition at the last page

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**4.Restart Seas:**

Go to <seas\_install>/bin and run the below commands:

$ ./stopSeas.sh mode=auto

$ ./startSeas.sh

**5.Okta settings to enable username instead of mail address:**

Login to okta and go Okta Developer > Directory > Profile Editor

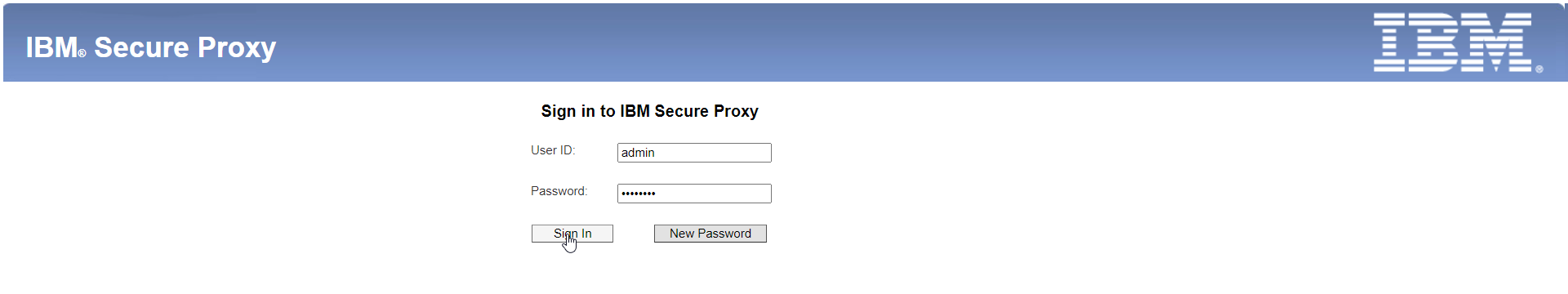
In Username(login) row click on info button and choose format restrictions to None (in place of email format)

A screenshot of a computer

Description automatically generated with medium confidence

**6.Use the Authentication Profile in SSPCM Policy and do the test:**

Login to SSPCM and to the policy(Policy we for integration of Okta)



Go to Configuration🡪 Policies and click on the respective policy and go to advanced page

Use the Authentication Profile name in the **External Authentication Profile** and click save.

A screenshot of a computer

Description automatically generated

After the configs are pushed to SSP Engines, we can try to connect to SFTP/MFG using the respective ports or URLs

**Note**: The user/partner we are trying to connect to SFTP/MFG should exists in Okta and SFG.