RSA Via L&G Collector Data Sheet
for
Oracle Identity Manager
Version 11.1.2.0.0 (Release 2)

Table of Contents

Purpose

This datasheet provides the configuration information required to create a new Oracle Identity Manager Version 2 collector.

Supported Software

RSA Via L&G Version: 6.9.1 *and above*

Application: Oracle Identity Manager Release 2

Collector Types: Identity Data Collector (IDC), Account Data Collector (ADC), Entitlement Data Collector (EDC), Role Data Collector (RDC)

Identity Data Collector

Prerequisites

Note: OIM_HOME is placeholder for the directory where OIM is installed.

Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download opensource jar file **xercesImpljaxb.jar (Applicable only for RSA Via L&G Version 7.0.0 and above)**

> Note:
>
> If wlfullclient.jar file is not present on specified location, you will have to generate it using following steps:
>
> 1. Open a command prompt and change directory to WL_HOME/server/lib: cd %WL_HOME%/server/lib
>
> 2. Use the following command to create wlfullclient.jar in the WL_HOME/server/lib directory: **java -jar wljarbuilder.jar**
>
> 3. You can now download wlfullclient.jar.

For consuming OIM Client APIs, JAAS related configurations are required:

JBOSS [For RSA Via L&G: 6.9.1 and Patch Versions]

1. Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200IdentityCollector1/lib

2. Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/APP-INF/lib
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200IdentityCollector1/lib

3. Add following JAAS configuration in ${JBOSS_HOME}/server/default/deploy/aveksa.ear/security.sar/META-INF/config/login-config.xml file:

```
<application-policy name="xellerate">
        <authentication>
                <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>
        </authentication>
</application-policy>
```

WildFly [For RSA Via L&G: 7.0 and above]

1. Modification in $<Wildfly_Home>\standalone/configuration/aveksa-standalone-full.xml
   Default Wildfly home for linux is /home/oracle/wildfly

   Adding a security domain :

   - Locate this
     <subsystem xmlns="urn:jboss:domain:security:1.2">

     <security-domains>

     </security-domains>

     </subsystem>
   - Add this following content in between the security-domains tags
     <security-domain name="xellerate">

     <authentication>

     <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>

     </authentication>

     </security-domain>

2. Create a new folder
   - mkdir /tmp/aveksa.ear
3. Unzip aveksa.ear to /tmp/aveksa.ear
   - unzip -q -X /tmp/repackaged_ear_dir/aveksa.ear -d /tmp/aveksa.ear
4. Copy downloaded wlfullclient.jar file to
   - /tmp/aveksa.ear/APP-INF/lib
   - /tmp/aveksa.ear/aveksa.war/OIM111200IdentityCollector1/lib
5. Copy the wlclient.jar file to
   - /tmp/aveksa.ear/aveksa.war**/**OIM111200IdentityCollector1/lib

Note: *Please refer the known issues before performing above step No.6

6. Copy xercesImpljaxb.jar file (a open source jar) to
   - /tmp/aveksa.ear/APP-INF/lib

7. Modification in /tmp/aveksa.ear/aveksa.war/WEB-INF/jboss-web.xml
    - Locate this

      <jboss-web>

      </jboss-web>

    - Add following content in between the tags

      <security-domain>java:/jaas/xellerate</security-domain>

8. Repackage the aveksa.ear after step 7 is completed.

   cd /tmp/aveksa.ear

   zip -q -r -u /home/oracle/aveksa.ear *

9. Restart the server.

   service aveksa_server restart

10. Undeploying aveksa.ear

    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="undeploy aveksa.ear"

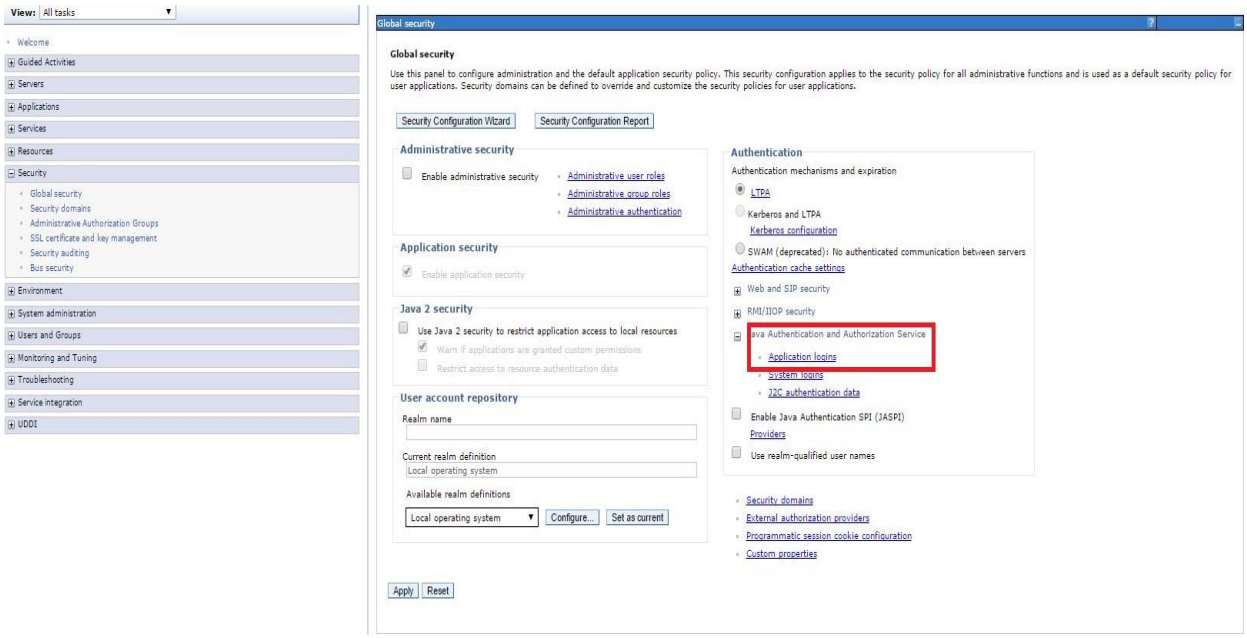
11. Deploying aveksa.ear

    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"

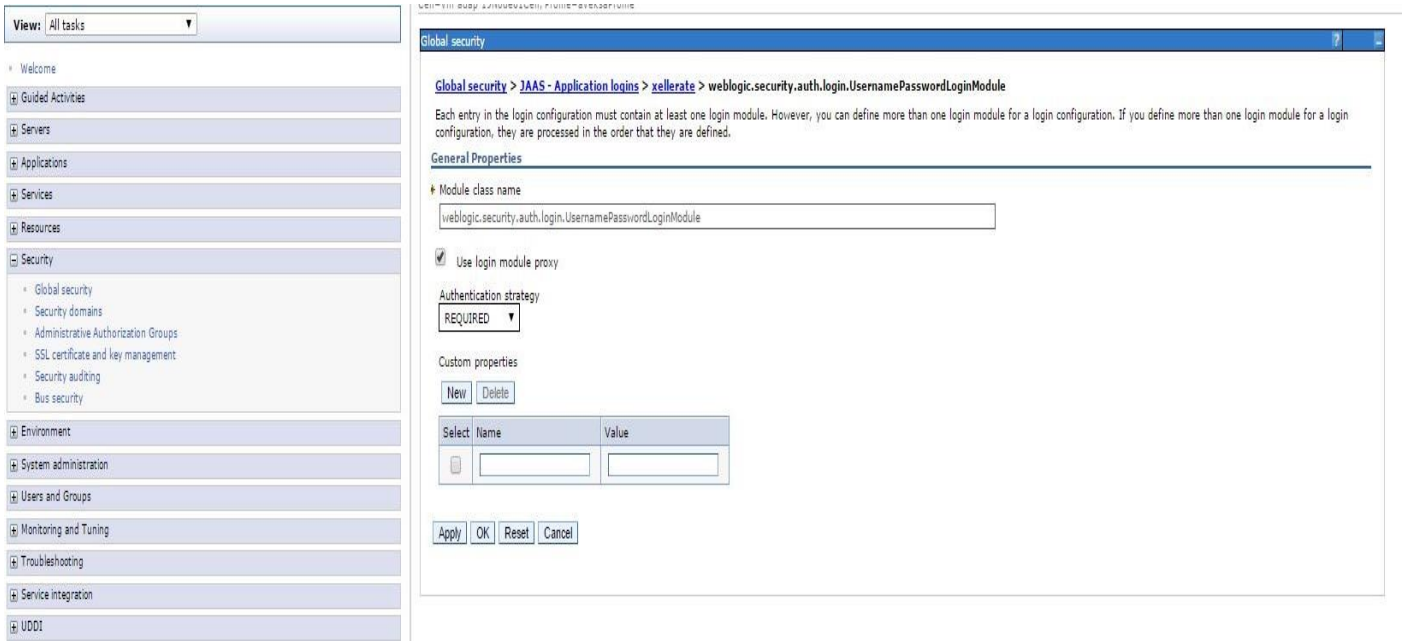
12. Delete the temporary directory /tmp/aveksa.ear

WebSphere [For RSA Via L&G: 6.9.1 and above]

1. Login to WebSphere admin console.
2. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.



3. Click ‘New’ to add new Login module.
4. Enter the ‘Alias’ as **xellerate**.
5. In JAAS login modules : Click ‘New’ to add the module class name.
6. Enter ‘Module class name’ as **weblogic.security.auth.login.UsernamePasswordLoginModule.**
7. Check the ‘Use login module proxy’ checkbox.
8. Select the ‘Authentication strategy’ as **Required**.



9. Click ‘Apply’ and ‘OK’.
10. Save the changes to master configuration.
11. Add the wlfullclient.jar at following locations :
    - $<aveksa.ear>/APP-INF/lib

- $<aveksa.ear>/aveksa.war/OIM111200IdentityCollector1/lib

e.g Default aveksa.ear file path for WAS :
/opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<Host_Name>Node01Cell/aveksa.ear/

12. Add wlclient.jar at following location :
    - $<aveksa.ear>/aveksa.war/OIM111200IdentityCollector1/lib
13. Restart the WAS Server using following command.
    /home/oracle/AFX/afx stop
    /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
    /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
    /home/oracle/AFX/afx start

Privileges required for Service Account

ACM & AFX applications need to access OIM using the OIM Client APIs and therefore require an authenticated session. Create a special user (integration user) in the OIM, solely for integration purposes. This will ensure that, even if an actual user is removed from the system, there will always be a user with the correct permissions available.

Add this user as a member of the following role:

- "Administrators"

Configuration

The configuration of the Identity data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen, while creating the Collector.

Field Name	**Value**
Collector Name	OIM Identity Data Collector
Description	OIM Identity Data Collector for version 11.1.2.0.0
Data Source Type	Oracle Identity Manager Ver. 11.1.2.0.0
Agent	AveksaAgent
Directory	Directory name under which Identity Data Collector is being created e.g. OIM_R2.

Status	Active
Copy from	Select already created OIM R2 IDC collector If you want to copy details from it.
Scheduled	Select Yes if you want to schedule collector.

Configuration Information

The following table lists the parameters on the "Configuration Information" screen, while creating the Collector.

Field Name	**Value**
OIM Url	URL of the App Server where OIM is deployed. For example, t3://<SERVER_HOST>:14000
OIM Username	Login Id of the user created for integration
OIM Password	Password for the user created for integration
Context Factory	Context Factory used to initialize the connection to OIM. (Default: weblogic.jndi.WLInitialContextFactory)
Configuration file	Path to the authentication configuration file containing authentication module details. (Optional)

Map Collector Attributes to Group Attributes

The following table lists the parameters on the "Map Collector Attributes to Group Attributes" screen, while creating the Collector.

Field Name	**Value**
OWNER	<KEEP VALUE AS BLANK>

Map Collector Attributes to User Attributes

The following table lists the parameters on the “Map Collector Attributes to User Attributes” screen, while creating the Collector.

Field Name	**Value**
First Name	First Name
Last Name	Last Name
User Id	User Login
Department	Organization Name
Email Address	Email
Job Status	Status

Attribute Evaluation

Field Name	**Value**
Business Unit Id	NAME

Known Issues

- For the OIM Collector to work, the xercesImpljaxb.jar has to be in placed at the location mentioned - Pre-requisites->JAAS configuration->For WildFly server->Step 5
  However, Once this jar is added, the "Reports" module within RSA-IMG cannot be used.
  With this limitation, either OIM Collector or the Reports Module will work at a time.

Account Data Collector

Prerequisites

Note: OIM_HOME is placeholder for the directory where OIM is installed.

Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download opensource jar file **xercesImpljaxb.jar (Applicable for RSA Via L&G Version 7.0.0 and above)**

> Note:
>
> If wlfullclient.jar file is not present on specified location, you will have to generate it using following steps:
>
> 1. Open a command prompt and change directory to WL_HOME/server/lib: cd %WL_HOME%/server/lib
>
> 2. Use the following command to create wlfullclient.jar in the WL_HOME/server/lib directory: **java -jar wljarbuilder.jar**
>
> 3. You can now download wlfullclient.jar.

For consuming OIM Client APIs, JAAS related configurations are required:

JBOSS [For RSA Via L&G: 6.9.1 and Patch Versions.]

1. Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:

   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200AccountCollector1/lib

2. Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:

   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200AccountCollector1/lib
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/APP-INF/lib

3. Add following JAAS configuration in ${JBOSS_HOME}/server/default/deploy/aveksa.ear/security.sar/META-INF/config/login-config.xml file:

```
<application-policy name="xellerate">
        <authentication>
                <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>
        </authentication>
</application-policy>
```

WildFly WebServer: [For RSA Via L&G: 6.9.1 and above]

1. Modification in $<Wildfly_Home>/standalone/configuration/aveksa-standalone-full.xml

Default Wildfly home for linux is /home/oracle/wildfly

Adding a security domain:

- Locate this
  <subsystem xmlns="urn:jboss:domain:security:1.2">

  <security-domains>

  </security-domains>

  </subsystem>
- Add this following content in between the security-domains tags
  <security-domain name="xellerate">

  <authentication>

  <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>

  </authentication>

  </security-domain>

2. Create a new folder
   mkdir /tmp/aveksa.ear
3. Unzip aveksa.ear to /tmp/aveksa.ear
   unzip -q -X /tmp/repackaged_ear_dir/aveksa.ear -d /tmp/aveksa.ear
4. Copy downloaded wlfullclient.jar file to
   - /tmp/aveksa.ear/APP-INF/lib
   - /tmp/aveksa.ear/aveksa.war/OIM111200AccountCollector1/lib
5. Copy the wlclient.jar file to
   - /tmp/aveksa.ear/aveksa.war**/**OIM111200AccountCollector1/lib

Note: *Please refer the known issues before performing above step No.6

6. Copy xercesImpljaxb.jar file (a open source jar) to

- /tmp/aveksa.ear/APP-INF/lib

7. Modification in /tmp/aveksa.ear/aveksa.war/WEB-INF/jboss-web.xml
   - Locate this

     <jboss-web>

     </jboss-web>

   - Add following content in between the tags

     <security-domain>java:/jaas/xellerate</security-domain>

8. Repackage the aveksa.ear after 7 is completed.
   cd /tmp/aveksa.ear

   zip -q -r -u /home/oracle/aveksa.ear *

9. Restart the server.
   service aveksa_server restart

10. Undeploying aveksa.ear

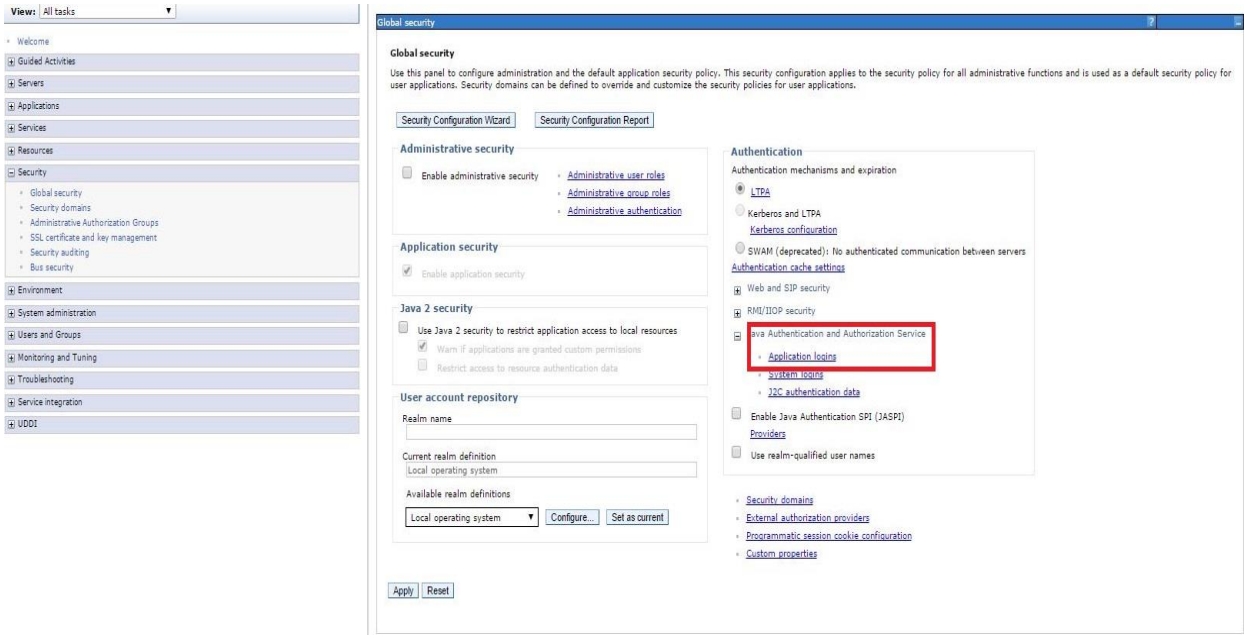
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="undeploy aveksa.ear"

11. Deploying aveksa.ear
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"

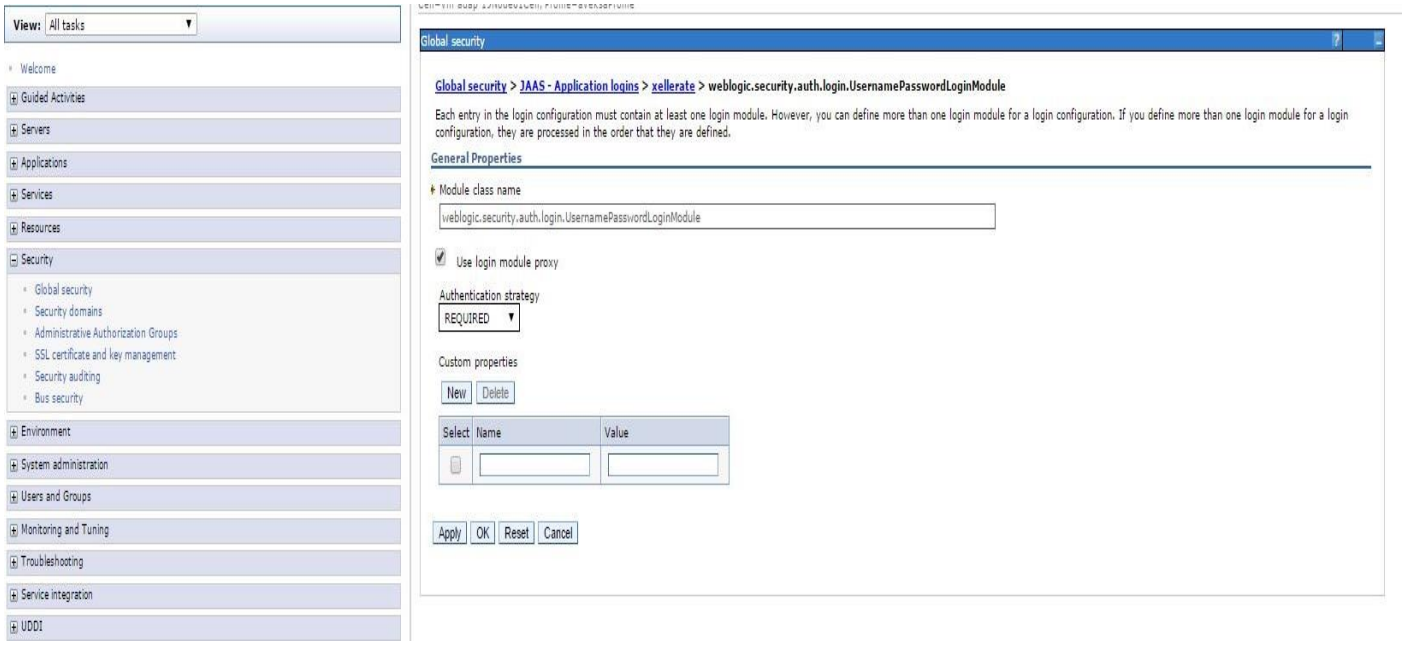
12. Delete the temporary directory /tmp/aveksa.ear

WebSphere Application Server: [For RSA Via L&G: 6.9.1 and above]

1. Login to WebSphere admin console.
2. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.



3. Click ‘New’ to add new Login module.
4. Enter the ‘Alias’ as **xellerate**.
5. In JAAS login modules: Click ‘**New**’ to add the module class name.
6. Enter ‘Module class name’ as **weblogic.security.auth.login.UsernamePasswordLoginModule.**
7. Check the ‘**Use login module proxy’** checkbox.
8. Select the ‘Authentication strategy’ as **Required**.



9. Click **‘Apply’** and ‘**OK**’.
10. Save the changes to master configuration.
11. Add the wlfullclient.jar at following locations :

- $<aveksa.ear>/APP-INF/lib
- $<aveksa.ear>/aveksa.war/OIM111200AccountCollector1/lib

e.g Default aveksa.ear file path for WAS :
/opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<Host_Name>Node01Cell/aveksa.ear/

12. Add wlclient.jar at following location :
    - $<aveksa.ear>/aveksa.war/OIM111200AccountCollector1/lib
13. Restart the WAS Server using following command.
    /home/oracle/AFX/afx stop
    /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
    /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
    /home/oracle/AFX/afx start

Privileges required for Service Account

ACM & AFX applications need to access OIM using the OIM Client APIs and therefore require an authenticated session. Create a special user (integration user) in the OIM, solely for integration purposes. This will ensure that, even if an actual user is removed from the system, there will always be a user with the correct permissions available.

Add this user as a member of the following role:

- "Administrators"

Configuration

The configuration of the Account data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen, while creating the Collector.

Field Name	**Value**
Collector Name	OIM Account Data Collector
Description	OIM Account Data Collector for version 11.1.2.0.0
Data Source Type	Oracle Identity Manager Ver. 11.1.2.0.0
Agent	AveksaAgent
Business Source	Directory name under which Account Data Collector is being created e.g. OIM_R2.

Status	Active
Copy from	Select already created OIM R2 ADC Collector If you want to copy details from it.
Scheduled	Select Yes if You want to Schedule Collector.

Configuration Information

The following table lists the parameters on the "Configuration Information" screen, while creating the Collector.

Field Name	**Value**
OIM Url	URL of the App Server where OIM is deployed. For example, t3://<SERVER_HOST>:14000
OIM Username	Login Id of the user created for integration
OIM Password	Password for the user created for integration
Context Factory	Context Factory used to initialize the connection to OIM. (Default: weblogic.jndi.WLInitialContextFactory)
Configuration file	Path to the authentication configuration file containing authentication module details. (Optional)

Map Collector Attributes to Account Attributes

The following table lists the parameters on the "Map Collector Attributes to Account Attributes" screen, while creating the Collector.

Field Name	**Value**
Last Login Date	<LEAVE BLANK>
Expiration Date	<LEAVE BLANK>

Map Collector Attributes to Account Mapping Attributes

The following table lists the parameters on the “Map Collector Attributes to Account Mapping Attributes” screen, while creating the Collector.

Field Name	**Value**
User Reference	USER_KEY

User Resolution Rules

Field Name	**Value**
Target Collector	OIM Identity Collector
User Attribute	User Id

Member Account Resolution

Field Name	**Value**
Target Collector	OIM Identity Collector
Account Attribute	Account Name

Known Issues

- For the OIM Collector to work, the xercesImpljaxb.jar has to be in placed at the location mentioned - Pre-requisites->JAAS configuration->For WildFly server->Step 5
  However, Once this jar is added, the "Reports" module within RSA-IMG cannot be used.
  With this limitation, either OIM Collector or the Reports Module will work at a time.

Entitlement Data Collector

Prerequisites

Note: OIM_HOME is placeholder for the directory where OIM is installed.

Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download opensource jar file **xercesImpljaxb.jar (Applicable for RSA Via L&G Version 7.0.0 and above)**

> Note:
>
> If wlfullclient.jar file is not present on specified location, you will have to generate it using following steps:
>
> 1. Open a command prompt and change directory to WL_HOME/server/lib: cd %WL_HOME%/server/lib
>
> 2. Use the following command to create wlfullclient.jar in the WL_HOME/server/lib directory: **java -jar wljarbuilder.jar**
>
> 3. You can now download wlfullclient.jar.

For consuming OIM Client APIs, JAAS related configurations are required:

JBOSS [For RSA Via L&G: 6.9.1 and Patch Versions.]

1. Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:

   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200EntitlementCollector1/lib
2. Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/APP-INF/lib
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200EntitlementCollector1/lib
3. Add following JAAS configuration in ${JBOSS_HOME}/server/default/deploy/aveksa.ear/security.sar/META-INF/config/login-config.xml file:

```
<application-policy name="xellerate">
        <authentication>
                <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>
        </authentication>
</application-policy>
```

WildFly [For RSA Via L&G: 7.0 and above]

1. Modification in $<Wildfly_Home>/standalone/configuration/aveksa-standalone-full.xml
   Default Wildfly home for linux is /home/oracle/wildfly

   Adding a security domain :

   - Locate this
     <subsystem xmlns="urn:jboss:domain:security:1.2">

     <security-domains>

     </security-domains>

     </subsystem>

   - Add this following content in between the security-domains tags
     <security-domain name="xellerate">

     <authentication>

     <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>

     </authentication>

     </security-domain>

2. Create a new folder
   `mkdir /tmp/aveksa.ear`

3. Unzip aveksa.ear to /tmp/aveksa.ear
   `unzip -q -X /tmp/repackaged_ear_dir/aveksa.ear -d /tmp/aveksa.ear`

4. Copy downloaded wlfullclient.jar file to
   - /tmp/aveksa.ear/APP-INF/lib
   - /tmp/aveksa.ear/aveksa.war/OIM111200EntitlementCollector1/lib
5. Copy the wlclient.jar file to
   - /tmp/aveksa.ear/aveksa.war/OIM111200EntitlementCollector1/lib

   Note: *Please refer the known issues before performing above step No.6

6. Copy xercesImpljaxb.jar file (a open source jar) to
   - /tmp/aveksa.ear/APP-INF/lib

7. Modification in /tmp/aveksa.ear/aveksa.war/WEB-INF/jboss-web.xml
   - Locate this

     <jboss-web>

     </jboss-web>

   - Add following content in between the tags

     <security-domain>java:/jaas/xellerate</security-domain>

8. Repackage the aveksa.ear after step 6 is completed.
   cd /tmp/aveksa.ear

   ```
   zip -q -r -u /home/oracle/aveksa.ear *
   ```

9. Restart the server.
   service aveksa_server restart

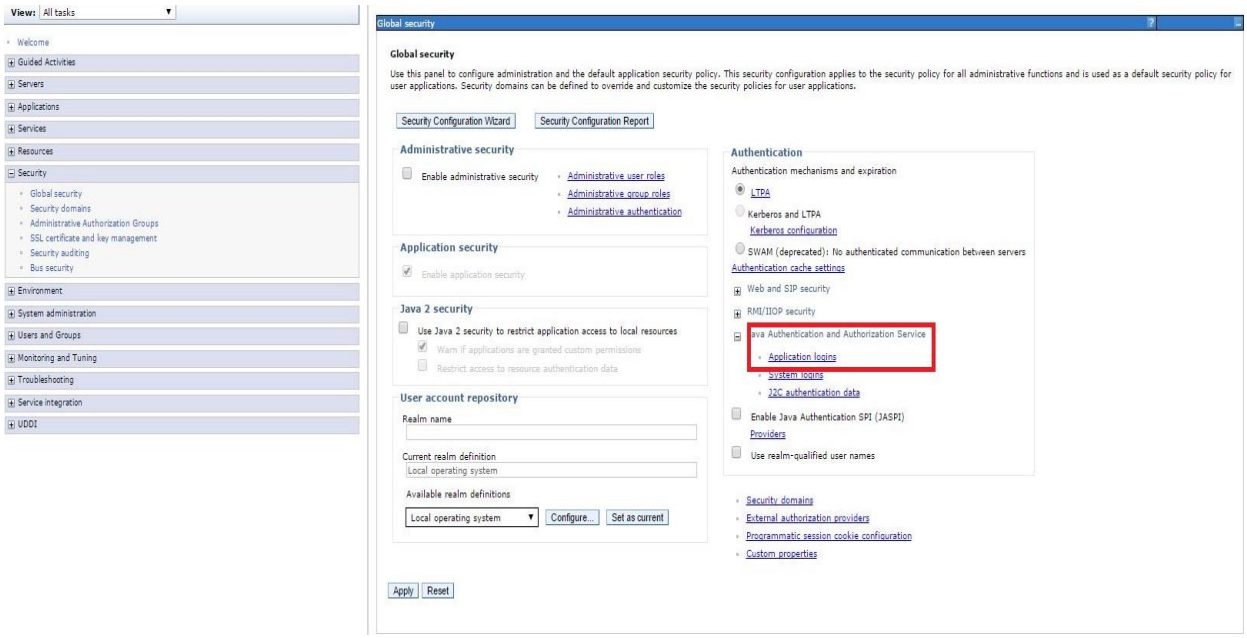
10. Undeploying aveksa.ear
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="undeploy aveksa.ear"

11. Deploying aveksa.ear
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"

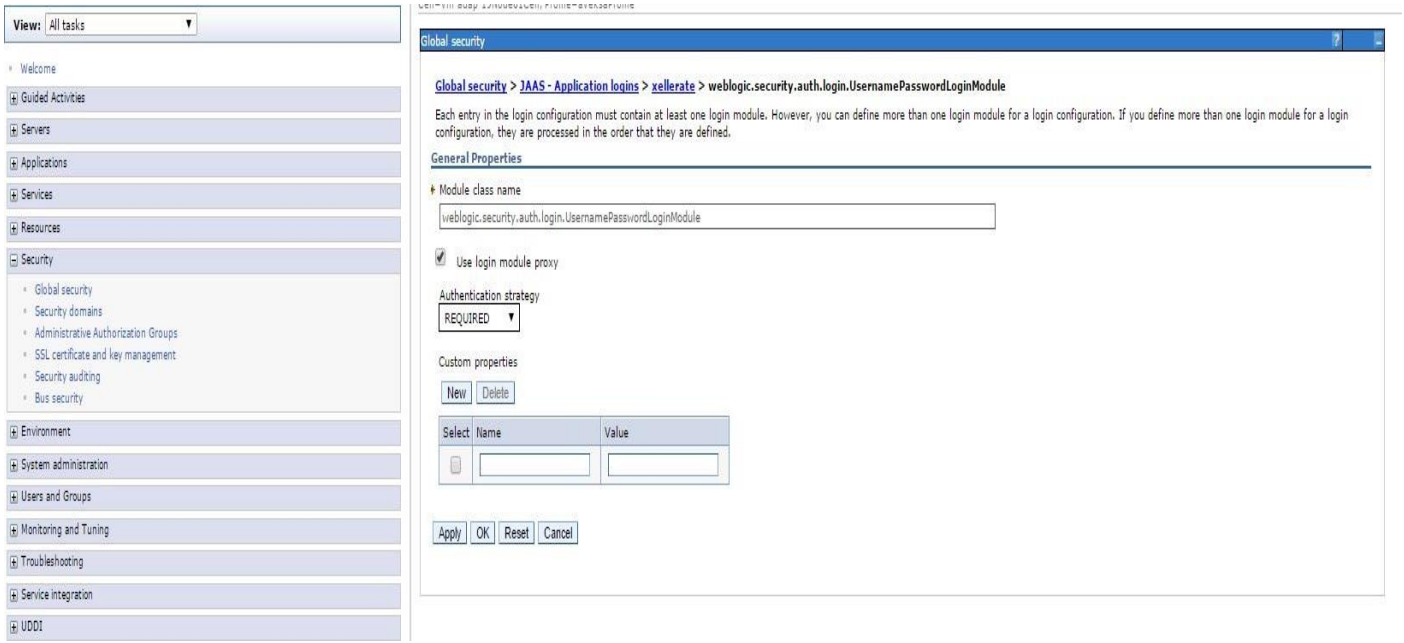
12. Delete the temporary directory /tmp/aveksa.ear

WebSphere Application Server: [For RSA Via L&G: 6.9.1 and above]

1. Login to WebSphere admin console.
2. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.



3. Click ‘New’ to add new Login module.
4. Enter the ‘Alias’ as **xellerate**.
5. In JAAS login modules : Click ‘New’ to add the module class name.
6. Enter ‘Module class name’ as **weblogic.security.auth.login.UsernamePasswordLoginModule.**
7. Check the ‘Use login module proxy’ checkbox.
8. Select the ‘Authentication strategy’ as **Required**.



9. Click ‘Apply’ and ‘OK’.

10. Save the changes to master configuration.
11. Add the wlfullclient.jar at following locations :
    - $<aveksa.ear>/APP-INF/lib
    - $<aveksa.ear>/aveksa.war/OIM111200EntitlementCollector1/lib

    e.g Default aveksa.ear file path for WAS :
    /opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<Host_Name>Node01Cell/aveksa.ear/
12. Add wlclient.jar at following location :
    - $<aveksa.ear>/aveksa.war/OIM111200EntitlementCollector1/lib
13. Restart the WAS Server using following command.

    /home/oracle/AFX/afx stop
    /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
    /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
    /home/oracle/AFX/afx start

Privileges required for Service Account

ACM & AFX applications need to access OIM using the OIM Client APIs and therefore require an authenticated session. Create a special user (integration user) in the OIM, solely for integration purposes. This will ensure that, even if an actual user is removed from the system, there will always be a user with the correct permissions available.

Add this user as a member of the following role:

- "Administrators"

Configuration

The configuration of the Entitlement data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen, while creating the Collector.

Field Name	**Value**
Collector Name	OIM Entitlement Data Collector
Description	OIM Entitlement Data Collector for version 11.1.2.0.0
Data Source Type	Oracle Identity Manager Ver. 11.1.2.0.0

Agent	AveksaAgent
Business Source	Directory name under which Entitlement Data Collector is being created e.g. OIM_R2.
Status	Active
Copy from	Select already created OIM R2 EDC collector If you want to copy details from it.
Scheduled	Select “Yes” if you want to schedule collector.

Configuration Information

The following table lists the parameters on the “Configuration Information” screen, while creating the Collector.

Field Name	**Value**
OIM Url	URL of the App Server where OIM is deployed. For example, t3://<SERVER_HOST>:14000
OIM Username	Login Id of the user created for integration
OIM Password	Password for the user created for integration
Context Factory	Context Factory used to initialize the connection to OIM. (Default: weblogic.jndi.WLInitialContextFactory)
Configuration file	Path to the authentication configuration file containing authentication module details. (Optional)

Account Evaluation Page

Field Name	**Value**
Associated account collector	OIM Account Collector
Account value	Account Name

Known Issues

- For the OIM Collector to work, the xercesImpljaxb.jar has to be in placed at the location mentioned - Pre-requisites->JAAS configuration->For WildFly server->Step 5
  However, Once this jar is added, the "Reports" module within RSA-IMG cannot be used.
  With this limitation, either OIM Collector or the Reports Module will work at a time.

Role Data Collector

Prerequisites

Note: OIM_HOME is placeholder for the directory where OIM is installed.

Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib***

Download opensource jar file **xercesImpljaxb.jar (Applicable for RSA Via L&G Version 7.0.0 and above)**

> Note:
>
> If wlfullclient.jar file is not present on specified location, you will have to generate it using following steps:
>
> 1. Open a command prompt and change directory to WL_HOME/server/lib: cd %WL_HOME%/server/lib
>
> 2. Use the following command to create wlfullclient.jar in the WL_HOME/server/lib directory: **java -jar wljarbuilder.jar**
>
> 3. You can now download wlfullclient.jar.

For consuming OIM Client APIs, JAAS related configurations are required:

JBOSS [For RSA Via L&G: 6.9.1 and Patch Versions.]

1. Download ***wlclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200RoleCollector1/lib
2. Download ***wlfullclient.jar*** *from* ***<OIM_HOME>/Middleware/wlserver_10.3/server/lib*** and copy it to following locations:
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/APP-INF/lib
   <JBOSS_HOME>/server/default/deploy/aveksa.ear/aveksa.war/OIM111200RoleCollector1/lib

3. Add following JAAS configuration in ${JBOSS_HOME}/server/default/deploy/aveksa.ear/security.sar/META-INF/config/login-config.xml file:

```
<application-policy name="xellerate">
        <authentication>
                <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>
        </authentication>
</application-policy>
```

WildFly [For RSA Via L&G: 7.0 and above]

1. Modification in $<Wildfly_Home>/standalone/configuration/aveksa-standalone-full.xml
   Default Wildfly home for linux is /home/oracle/wildfly

   Adding a security domain :

   - Locate this
     <subsystem xmlns="urn:jboss:domain:security:1.2">

     <security-domains>

     </security-domains>

     </subsystem>

   - Add this following content in between the security-domains tags
     <security-domain name="xellerate">

     <authentication>

     <login-module code="weblogic.security.auth.login.UsernamePasswordLoginModule" flag="required"/>

     </authentication>

     </security-domain>

2. Create a new folder
   `mkdir /tmp/aveksa.ear`

3. Unzip aveksa.ear to /tmp/aveksa.ear
   `unzip -q -X /tmp/repackaged_ear_dir/aveksa.ear -d /tmp/aveksa.ear`

4. Copy downloaded wlfullclient.jar file to
   - /tmp/aveksa.ear/APP-INF/lib
   - /tmp/aveksa.ear/aveksa.war/OIM111200RoleCollector1/lib
5. Copy the wlclient.jar file to
   - /tmp/aveksa.ear/aveksa.war**/**OIM111200RoleCollector1/lib

Note : *Please refer the known issues before performing below step 6.

6. Copy xercesImpljaxb.jar file (a open source jar) to
   - /tmp/aveksa.ear/APP-INF/lib

7. Modification in /tmp/aveksa.ear/aveksa.war/WEB-INF/jboss-web.xml
   - Locate this

<jboss-web>

</jboss-web>

- Add following content in between the tags
  <security-domain>java:/jaas/xellerate</security-domain>

8. Repackage the aveksa.ear after steps 7 is completed.
   cd /tmp/aveksa.ear

   zip -q -r -u /home/oracle/aveksa.ear *

9. Restart the server.
   service aveksa_server restart

10. Undeploying aveksa.ear

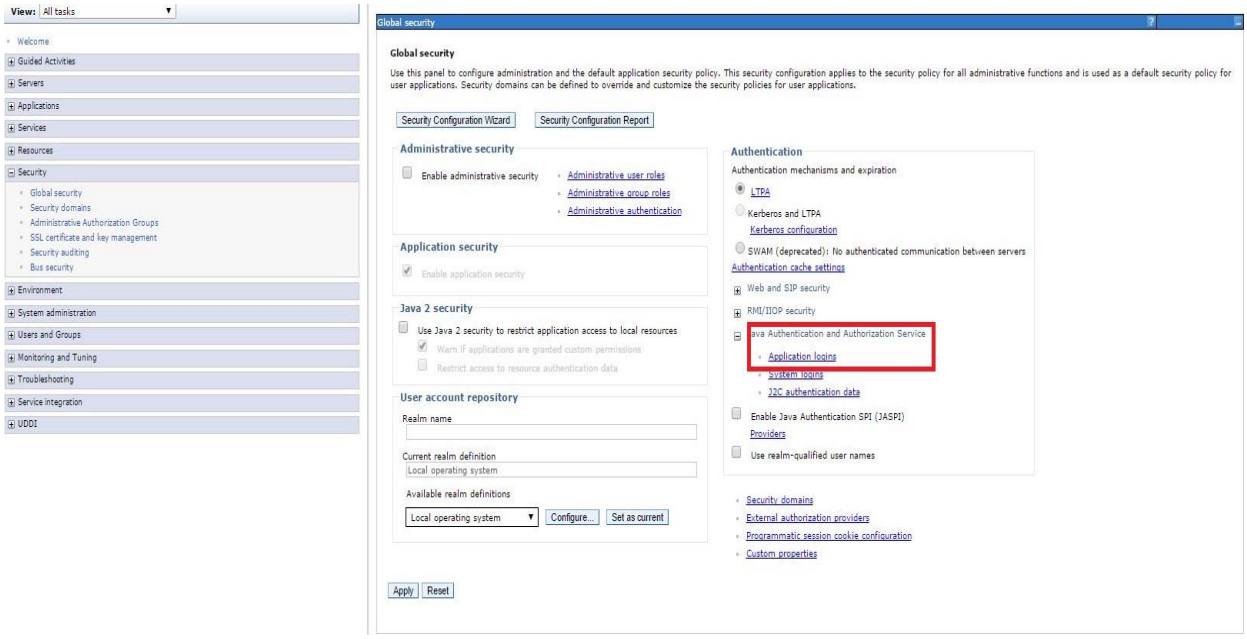
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="undeploy aveksa.ear"

11. Deploying aveksa.ear
    /home/oracle/wildfly/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"

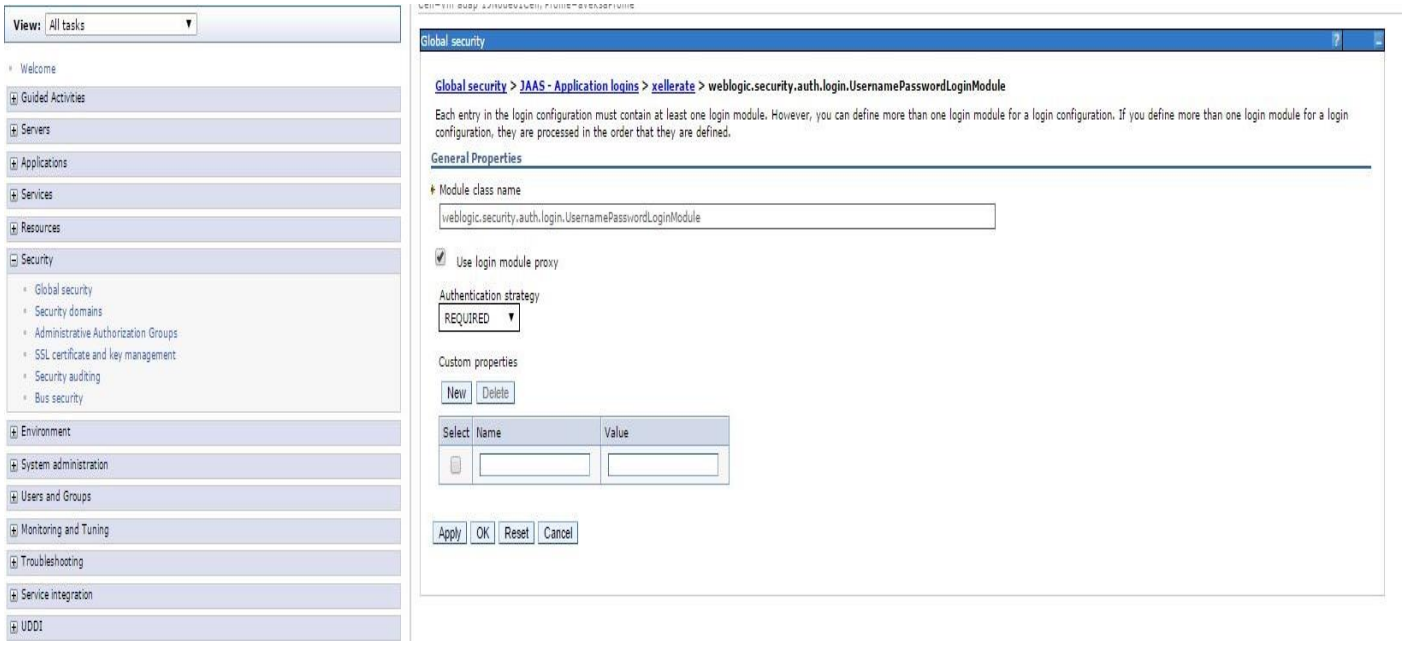
12. Delete the temporary directory /tmp/aveksa.ear

WebSphere Application Server: [For RSA Via L&G: 6.9.1 and above]

1. Login to WebSphere admin console.
2. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.



3. Click ‘New’ to add new Login module.
4. Enter the ‘Alias’ as **xellerate**.
5. In JAAS login modules: Click ‘New’ to add the module class name.
6. Enter ‘Module class name’ as **weblogic.security.auth.login.UsernamePasswordLoginModule.**
7. Check the ‘Use login module proxy’ checkbox.
8. Select the ‘Authentication strategy’ as **Required**.



9. Click ‘Apply’ and ‘OK’.
10. Save the changes to master configuration.
11. Add the wlfullclient.jar at following locations :

- $<aveksa.ear>/APP-INF/lib
- $<aveksa.ear>/aveksa.war/OIM111200RoleCollector1/lib

e.g Default aveksa.ear file path for WAS :
/opt/IBM/WebSphere/AppServer/profiles/aveksaProfile/installedApps/<Host_Name>Node01Cell/aveksa.ear/

12. Add wlclient.jar at following location :
    - $<aveksa.ear>/aveksa.war/ OIM111200RoleCollector1/lib
13. Restart the WAS Server using following command.

    /home/oracle/AFX/afx stop
    /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
    /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
    /home/oracle/AFX/afx start

Privileges required for Service Account

ACM & AFX applications need to access OIM using the OIM Client APIs and therefore require an authenticated session. Create a special user (integration user) in the OIM, solely for integration purposes. This will ensure that, even if an actual user is removed from the system, there will always be a user with the correct permissions available.

Add this user as a member of the following role:

- "Administrators"

Configuration

The configuration of the Role data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Collector Description

The following table lists the parameters on the “Collector Description” screen, while creating the Collector.

Field Name	**Value**
Collector Name	OIM Role Data Collector
Description	OIM Role Data Collector for version 11.1.1.3.0
Data Source Type	Oracle Identity Manager Ver. 11.1.1.3.0
Agent	AveksaAgent
Directory	Directory name under which Role Data Collector is being created e.g. OIM_R2.

Status	Active
Copy from	Select already created OIMR1 RDC Collector If you want to copy details from it.
Scheduled	Select Yes if You want to Schedule Collector.

Configuration Information

The following table lists the parameters on the “Configuration Information” screen, while creating the Collector.

Field Name	**Value**
OIM Url	URL of the App Server where OIM is deployed. For example, t3://<SERVER_HOST>:14000
OIM Username	Login Id of the user created for integration
OIM Password	Password for the user created for integration
Context Factory	Context Factory used to initialize the connection to OIM. (Default: weblogic.jndi.WLInitialContextFactory)
Configuration file	Path to the authentication configuration file containing authentication module details. (Optional)

User Evaluation

Field Name	**Value**
Owner	User Id
Role Member	User Id

Known Issues

- For the OIM Collector to work, the xercesImpljaxb.jar has to be in placed at the location mentioned - Pre-requisites->JAAS configuration->For WildFly server->Step 6
  However, Once this jar is added, the "Reports" module within RSA-IMG cannot be used.
  With this limitation, either OIM Collector or the Reports Module will work at a time.

Copyrights

Trademarks