

**RSA Via L&G Collector Data Sheet
for
Oracle Identity Manager (OIM)
Version 11.1.1.3.0 (Release 1)**



Table of Contents

Supported Software	3
Identity Data Collector	4
<i>Prerequisites</i>	4
<i>Configuration</i>	8
Collector Description	8
Configuration Information	9
Map Collector Attributes to User Attributes	9
Attribute Evaluation	10
<i>Known Issues</i>	10
Account Data Collector	11
<i>Prerequisites</i>	11
<i>Configuration</i>	16
Collector Description	16
Configuration Information	16
Map Collector Attributes to Account Attributes	17
Map Collector Attributes to Account Mapping Attributes	17
User Resolution Rules	17
Member Account Resolution	17
<i>Known Issues</i>	18
Entitlement Data Collector	19
<i>Prerequisites</i>	19
<i>Configuration</i>	24
Collector Description	24
Configuration Information	24
Account Evaluation Page	25
<i>Known Issues</i>	25
Role Data Collector	26
<i>Prerequisites</i>	26
<i>Configuration</i>	30
Collector Description	30
Configuration Information	31
User Evaluation	31
<i>Known Issues</i>	31

Purpose

This datasheet provides the configuration information required to create a new Oracle Identity Manager Release 1 Identity Data Collector, Account Data Collector, Entitlement Data Collector and Role Data Collector.

Supported Software

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

Application: Oracle Identity Manager Release 1

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

Download open source jar file **xercesImpljxb.jar**

Note:

If wfullclient.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 wfullclient.jar in the WL_HOME/server/lib directory: `java -jar wljarbuilder.jar`
3. You can now download wfullclient.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/OIM111130IdentityCollector1/lib`
2. Download **wfullclient.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/OIM111130IdentityCollector1/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 wfullclient.jar file to
 - /tmp/aveksa.ear/APP-INF/lib
 - /tmp/aveksa.ear/aveksa.war/ OIM111130IdentityCollector1/lib
5. Copy the wlclient.jar file to
 - /tmp/aveksa.ear/aveksa.war/OIM111130IdentityCollector1/lib
6. Copy xercesImpljxb.jar file (a open source jar) to
 - /tmp/aveksa.ear/APP-INF/lib

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

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 4, 5,6 and 7 are complete.

```
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"
```

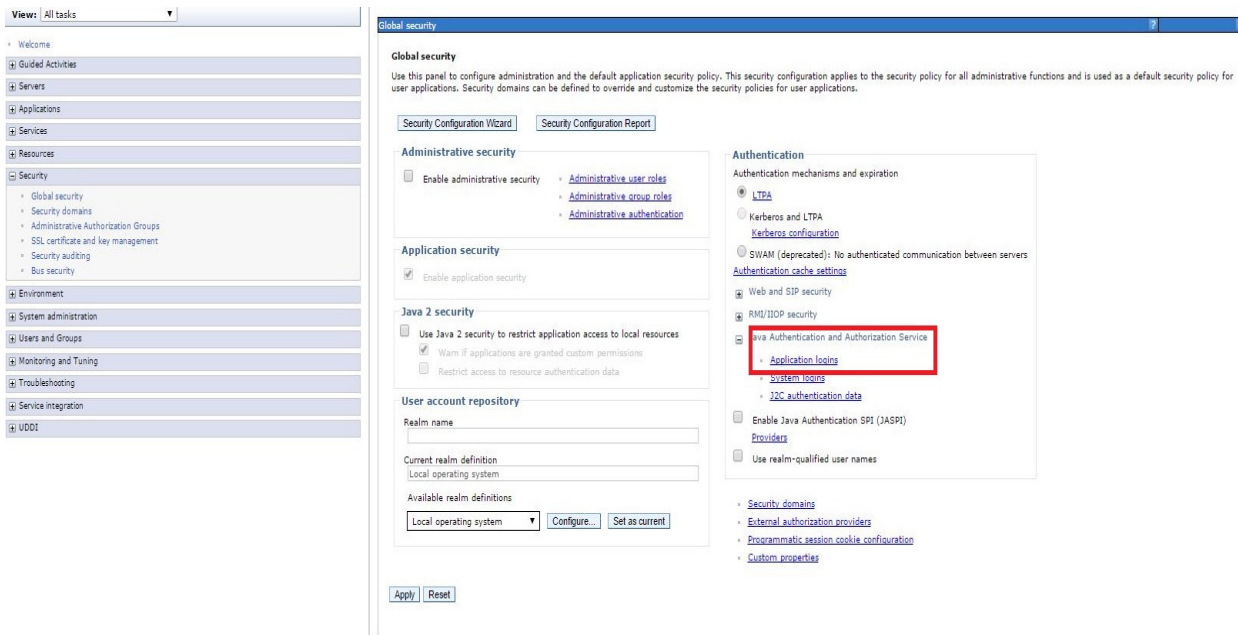
11. Deploying aveksa.ear

```
/home/oracle/wildfly-8.2.0.Final/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"
```

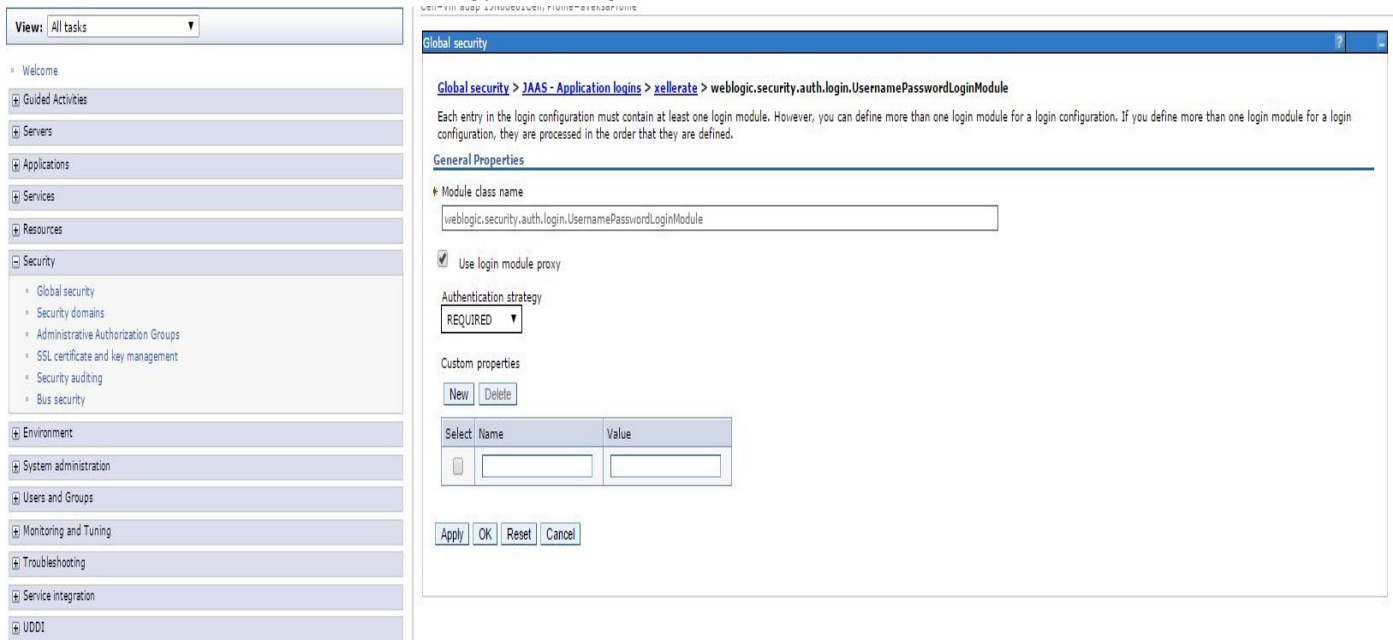
12. Delete the temporary directory /tmp/aveksa.ear

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 wifullclient.jar at following locations :

- \$<aveksa.ear>/APP-INF/lib
 - \$<aveksa.ear>/aveksa.war/OIM111130IdentityCollector1/lib
12. Add wlclient.jar at following location :
- \$<aveksa.ear>/aveksa.war/OIM111130IdentityCollector1/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 11.1.1.3.0                                                                           |
| Data Source Type | Oracle Identity Manager Ver. 11.1.1.3.0                                                                                      |
| Agent            | AveksaAgent                                                                                                                  |
| Directory        | Select already created Directory. If you have not created any directory then create any directory from Resource > Directory. |



|           |                                                                                 |
|-----------|---------------------------------------------------------------------------------|
| Status    | Active                                                                          |
| Copy from | Select already created OIMR1 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: <i>weblogic.jndi.WLInitialContextFactory</i> ) |
| Configuration file | Path to the authentication configuration file containing authentication module details. (Optional)                 |

### 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    | act_key |
| Email Address | Email   |
| Job Status    | Status  |

### *Attribute Evaluation*

| Field Name       | Value |
|------------------|-------|
| Business Unit Id | NAME  |

### *Known Issues*

- For the OIM Collector to work, the xercesImpljxb.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.

# 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 **xercesImpljxb.jar**

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. ]**

4. 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/OIM111130AccountCollector1/lib`

5. 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/OIM111130AccountCollector1/lib`  
`<JBOSS_HOME>/server/default/deploy/aveksa.ear/APP-INF/lib`

6. 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]**

13. 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>`

14. Create a new folder

`mkdir /tmp/aveksa.ear`

15. Unzip aveksa.ear to /tmp/aveksa.ear

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

16. Copy downloaded wfullclient.jar file to

- /tmp/aveksa.ear/APP-INF/lib
- /tmp/aveksa.ear/aveksa.war/OIM111130AccountCollector1/lib

17. Copy the wlclient.jar file to

- /tmp/aveksa.ear/aveksa.war/OIM111130AccountCollector1/lib

18. Copy xercesImpljxb.jar file (a open source jar) to

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

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

19. 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>`

20. Repackage the aveksa.ear after steps 4, 5 ,6 and 7 are complete.

```
cd /tmp/aveksa.ear
```

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

21. Restart the server.

```
service aveksa_server restart
```

22. Undeploying aveksa.ear

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

23. Deploying aveksa.ear

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

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

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

14. Login to WebSphere admin console.

15. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.

The screenshot shows the WebSphere Administration Console interface. The top navigation bar includes the WebSphere logo and the user name 'Welcome AvekshaAd'. The left sidebar contains a tree view of the console's structure, with 'Security' expanded and 'Global security' selected, indicated by a red arrow. The main content area displays the 'Global security' configuration page. It includes a 'Global security' header with a brief description and two buttons: 'Security Configuration Wizard' and 'Security Configuration Report'. Below this are several sections: 'Administrative security' with a checkbox for 'Enable administrative security' and links for 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'; 'Application security' with a checked checkbox for 'Enable application security'; 'Java 2 security' with checkboxes for 'Use Java 2 security to restrict application access to local resources', 'Warn if applications are granted custom permissions', and 'Restrict access to resource authentication data'; and 'User account repository' with input fields for 'Realm name' and 'Current realm definition'. On the right side, the 'Authentication' section is expanded, showing 'Authentication mechanisms and expiration' with radio buttons for 'LTPA' (selected), 'Kerberos and LTPA', and 'SWAM (deprecated)'. Below this are links for 'Kerberos configuration', 'Authentication cache settings', and 'Web and SIP security'. The 'Java Authentication and Authorization Service' section is also expanded, with 'Application logins' highlighted by a red arrow, and sub-links for 'System logins' and 'J2C authentication data'. Other options include 'Enable Java Authentication SPI (JASPI)', 'Providers', and 'Use realm-qualified user names'.

16. Click 'New' to add new Login module.
17. Enter the 'Alias' as **xellerate**.
18. In JAAS login modules : Click 'New' to add the module class name.
19. Enter 'Module class name' as **weblogic.security.auth.login.UsernamePasswordLoginModule**.
20. Check the 'Use login module proxy' checkbox.
21. Select the 'Authentication strategy' as **Required**.

WebSphere software

View: All tasks

Cell=vm-adap-19Node01Cell, Profile=aveksaProfile

Global security

Messages

- Changes have been made to your local configuration. You can:
  - Save directly to the master configuration.
  - Review changes before saving or discarding.
- The server may need to be restarted for these changes to take effect.

Global security > JAAS - Application logins > New... > New...

Each entry in the login configuration must contain at least one login module. However, you can define more than one login module for a login configuration, they are processed in the order that they are defined.

General Properties

\* Module class name  
weblogic.security.auth.login.UsernamePasswordLoginModule

Use login module proxy

Authentication strategy  
REQUIRED

Custom properties  
New Delete

Select	Name	Value
<input type="checkbox"/>		

Apply OK Reset Cancel

22. Click 'Apply' and 'OK'.
23. Save the changes to master configuration.
24. Add the wfullclient.jar at following locations :
  - \$<aveksa.ear>/APP-INF/lib
  - \$<aveksa.ear>/aveksa.war/OIM111130AccountCollector1/lib
25. Add wlclient.jar at following location :
  - \$<aveksa.ear>/aveksa.war/OIM111130AccountCollector1/lib
26. Restart the 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 11.1.1.3.0
Data Source Type	Oracle Identity Manager Ver. 11.1.1.3.0
Agent	AveksaAgent
Business Source	Select already Created OIM Directory. If You have not created any Directory then Create Any Directory from Resource > Directory.
Status	Active
Copy from	Select already created OIMR1 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: <i>weblogic.jndi.WLInitialContextFactory</i> )
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 Account Collector

Account Attribute	Account Name
-------------------	--------------

### *Known Issues*

- For the OIM Collector to work, the xercesImpljxb.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.

# 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 **wfullclient.jar** from **<OIM\_HOME>/Middleware/wlserver\_10.3/server/lib**

Download opensource jar file **xercesImpljxb.jar**

Note:

If wfullclient.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 wfullclient.jar in the WL\_HOME/server/lib directory: **java -jar wljarbuilder.jar**
3. You can now download wfullclient.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/OIM111130EntitlementCollector1/lib`
7. Download **wfullclient.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/OIM111130EntitlementCollector1/lib`
8. 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]

25. 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>
```

26. Create a new folder

```
mkdir /tmp/aveksa.ear
```

27. Unzip aveksa.ear to /tmp/aveksa.ear

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

28. Copy downloaded wfullclient.jar file to

- /tmp/aveksa.ear/APP-INF/lib
- /tmp/aveksa.ear/aveksa.war/OIM111130EntitlementCollector1/lib

29. Copy the wlclient.jar file to

- /tmp/aveksa.ear/aveksa.war/OIM111130EntitlementCollector1/lib

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

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

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

31. Modification in /tmp/aveksa.ear/aveksa.wa/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>

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

```
cd /tmp/aveksa.ear
```

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

33. Restart the server.

```
service aveksa_server restart
```

34. Undeploying aveksa.ear

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

35. Deploying aveksa.ear

```
/home/oracle/wildfly-8.2.0.Final/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"
```

36. 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.

The screenshot displays the WebSphere Administration Console interface. The top navigation bar includes the WebSphere logo and the user name 'Welcome AvekshaAd'. The left sidebar contains a tree view of system components, with 'Security' expanded and 'Global security' selected, indicated by a red arrow. The main content area is titled 'Global security' and provides instructions on configuring administration and application security. It features several configuration sections: 'Administrative security' with links for user and group roles; 'Application security' with an enabled checkbox; 'Java 2 security' with options for local resource access; and 'User account repository' with fields for realm name and definition. On the right, the 'Authentication' section is expanded to show 'Application logins', which is also highlighted by a red arrow. Other authentication options like LTPA, Kerberos, and SWAM are visible but not selected.

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**.

WebSphere software

View: All tasks

Cell=vm-adap-19Node01Cell, Profile=aveksaProfile

Global security

Messages

- ⚠ Changes have been made to your local configuration. You can:
  - [Save](#) directly to the master configuration.
  - [Review](#) changes before saving or discarding.
- ⚠ The server may need to be restarted for these changes to take effect.

Global security > JAAS - Application logins > New... > New...

Each entry in the login configuration must contain at least one login module. However, you can define more than one login module for a login configuration, they are processed in the order that they

General Properties

\* Module class name  
weblogic.security.auth.login.UsernamePasswordLoginModule

Use login module proxy

Authentication strategy  
REQUIRED

Custom properties  
New Delete

Select	Name	Value
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Apply OK Reset Cancel

9. Click 'Apply' and 'OK'.
10. Save the changes to master configuration.
11. Add the wfullclient.jar at following locations :
  - \$<aveksa.ear>/APP-INF/lib
  - \$<aveksa.ear>/aveksa.war/OIM111130EntitlementCollector1/lib
12. Add wlclient.jar at following location :
  - \$<aveksa.ear>/aveksa.war/OIM111130EntitlementCollector1/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 11.1.1.3.0
Data Source Type	Oracle Identity Manager Ver. 11.1.1.3.0
Agent	AveksaAgent
Business Source	Select already Created OIM Directory.If You have not created any Directory then Create Any Directory from Resource > Directory.
Status	Active
Copy from	Select already created OIM R1 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: <i>weblogic.jndi.WLInitialContextFactory</i> )
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 xercesImpljxb.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.

# 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 **wfullclient.jar** from **<OIM\_HOME>/Middleware/wlserver\_10.3/server/lib**

Download opensource jar file **xercesImpljxb.jar**

Note:

If wfullclient.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 wfullclient.jar in the WL\_HOME/server/lib directory: **java -jar wljarbuilder.jar**
3. You can now download wfullclient.jar.

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

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

9. 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/OIM111130RoleCollector1/lib**
10. Download **wfullclient.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/OIM111130RoleCollector1/lib**
11. 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]**

14. 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>
```

15. Create a new folder

```
mkdir /tmp/aveksa.ear
```

16. Unzip aveksa.ear to /tmp/aveksa.ear

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

17. Copy downloaded wfullclient.jar file to

- /tmp/aveksa.ear/APP-INF/lib
- /tmp/aveksa.ear/aveksa.war/OIM111130RoleCollector1/lib

18. Copy the wclient.jar file to

- /tmp/aveksa.ear/aveksa.war/OIM111130RoleCollector1/lib

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

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

20. 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>

21. Repackage the aveksa.ear after step 7 is complete.

```
cd /tmp/aveksa.ear
```

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

22. Restart the server.

```
service aveksa_server restart
```

23. Undeploying aveksa.ear

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

24. Deploying aveksa.ear

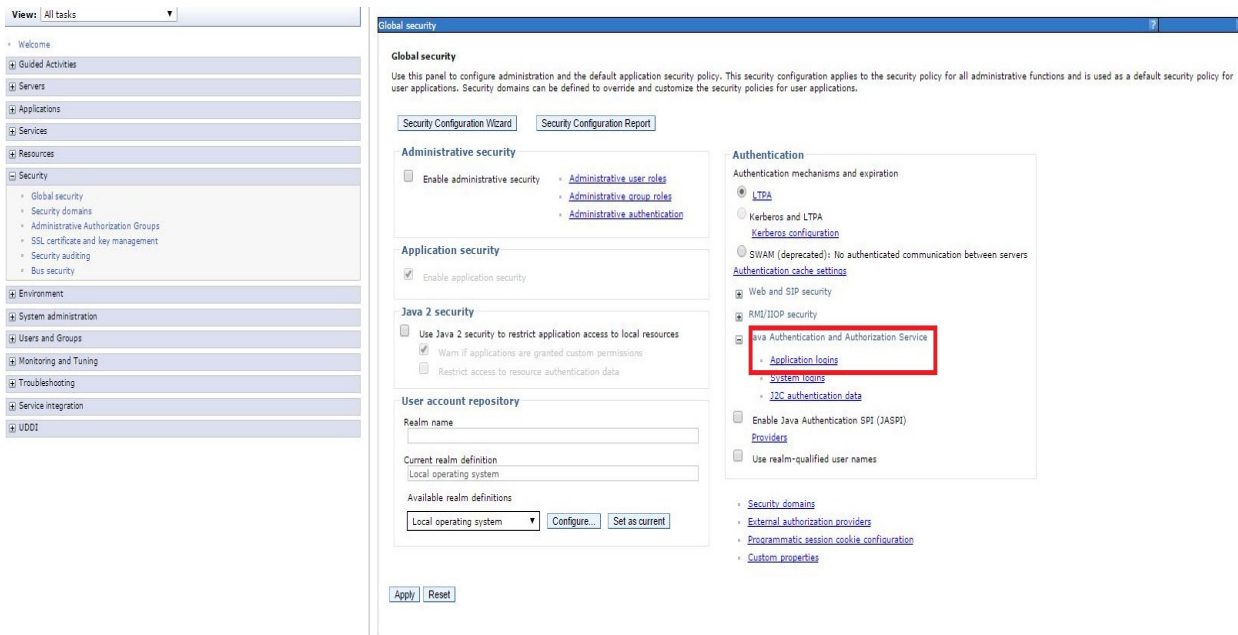
```
/home/oracle/wildfly-8.2.0.Final/bin/jboss-cli.sh -c --command="deploy /home/oracle/aveksa.ear --force"
```

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

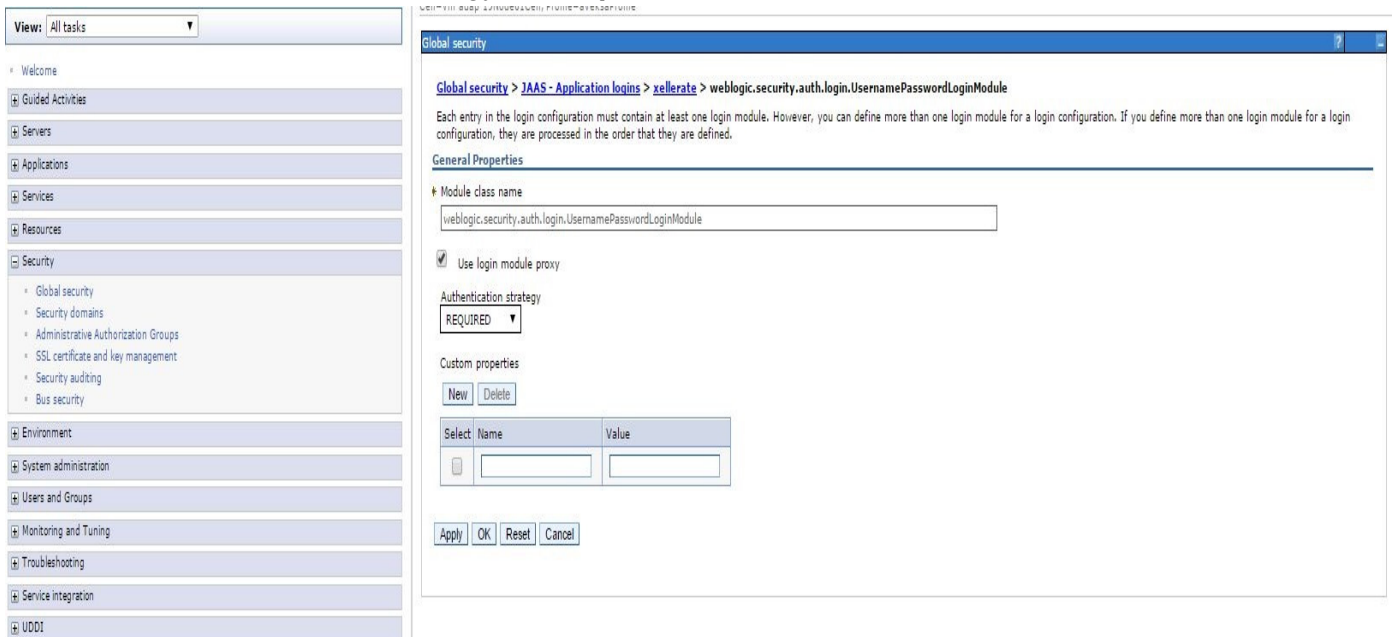
### **WebSphere Application Server: [For RSA Via L&G: 6.9.1 and above]**

26. Login to WebSphere admin console.

27. Navigate to Security-> Global security-> Java Authentication and Authorization Service-> Application logins.



28. Click 'New' to add new Login module.
29. Enter the 'Alias' as **xellerate**.
30. In JAAS login modules : Click 'New' to add the module class name.
31. Enter 'Module class name' as **weblogic.security.auth.login.UsernamePasswordLoginModule**.
32. Check the 'Use login module proxy' checkbox.
33. Select the 'Authentication strategy' as **Required**.



34. Click 'Apply' and 'OK'.
35. Save the changes to master configuration.
36. Add the wfullclient.jar at following locations :
  - $\$(aveksa.ear)/APP-INF/lib$

- \$<aveksa.ear>/aveksa.war/OIM111130RoleCollector1/lib
37. Add wlclient.jar at following location :
- \$<aveksa.ear>/aveksa.war/OIM111130RoleCollector1/lib
38. 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 | Select already Created OIM Directory. If You have not created any Directory then Create Any Directory from Resource > Directory. |
| 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: <i>weblogic.jndi.WLInitialContextFactory</i>) |
| 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 xercesImpljxb.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

Copyright © 2015 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.rsa.com/legal/trademarks_list.pdf.