Implementing Custom Security in Oracle Fusion Analytics Warehouse

FAW Product Management and Engineering

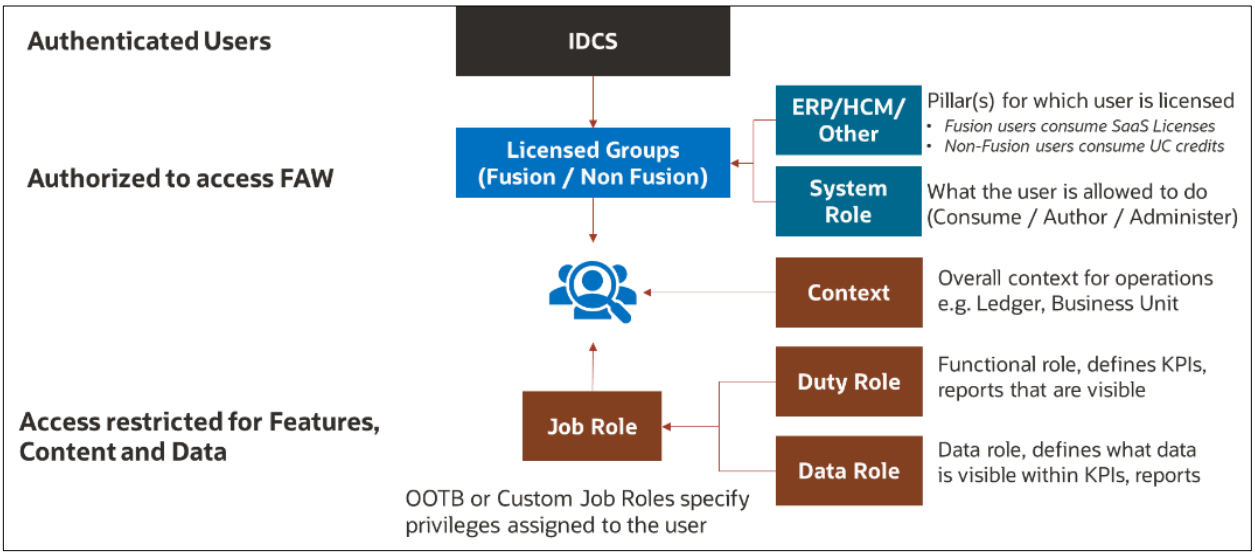
Introduction

Oracle Fusion Analytics Warehouse (FAW) delivers a robust security framework that protects your business data from unauthorized access, secures access to analytic objects based on the user's job functions and secures access to data they are allowed to view. The framework also provides you with the ability to view, create or administer objects in the semantic model.

Additionally, FAW offers you the ability to configure security according to your specific needs, beyond what is delivered out of the box. This document describes how you can configure data security to address more complex requirements.

Security Framework in FAW

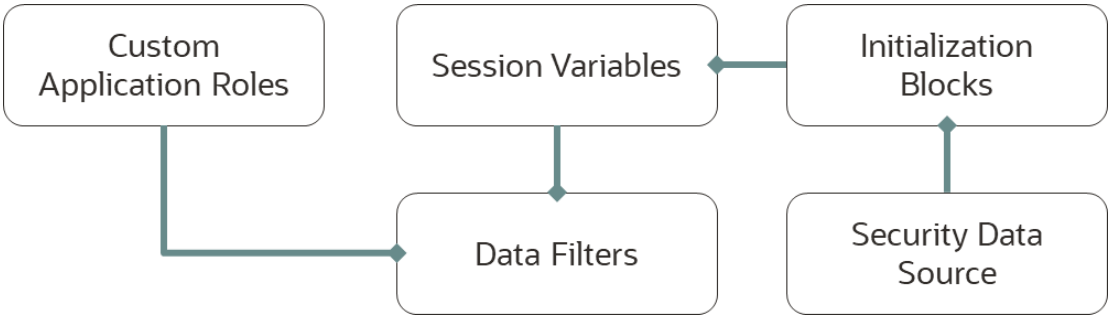
Figure 1 illustrates the basic security framework in FAW. FAW synchronizes users and groups from Fusion Cloud Applications. These users and groups are then associated with FAW Licensed Groups that allow you to access FAW's pre-built analytics. They also specify the user's system permissions (i.e.,



whether they can consume, author or administer content for a specific module). For example, users in the "FAW Licensed ERP Authors" group can create visualizations in FAW specific to ERP Analytics Subject Areas. Users are further constrained by their Job Roles, which in turn have Duty Roles and Data Roles. Duty Roles are tied to the functional responsibilities of the user and allow you to restrict access to specific Subject Areas, while Data Roles and Security Contexts help define the data access boundaries. For example, a user with the "Workforce Core Analysis" Duty Role and with the security context of the Business Unit defined as "California" will allow the user to see headcount and turnover data for the California Business Unit of the organization.

Advanced Data Security

FAW allows you to define advanced data security to meet more complex needs. Customers who want to override the data security delivered as part of the FAW implementation for specific users can take advantage of this capability. Data-level security in FAW is implemented in four basic steps:



1. Set up security assignments in a custom table that incorporate the desired security rules for the specific users. This is your custom security data source.
2. Set up session variables and initialization blocks that obtain specific security-related information when a user logs in. Initialization blocks obtain dimension members for each user session in order to restrict row-level access to data in facts or dimensions.
3. Set up desired custom Application Roles (data roles) and assign desired users and groups to these data roles.
4. Set up data filters that specify the values for specific dimensions that will be passed to the session variable for the . While defining data filters, you can use functional groups to further control how multiple data filters will be applied.

The following section shows an example of an advanced security implementation.

Example

In this example, we will take the case of the user Ravi Chouhan, a line manager who also needs to view data for his department, grade, or his own record. The following requirements need to be met:

- As a line manager, Ravi should have access to assignments within his reporting hierarchy and his own assignments.
- As an analyst, Ravi should have access to:
  - Person assignments from department = "BI_HR-Dept14-Business Visit Unit"
  - Grade: "BI_HR_IC3 - Individual Contributor Pay Grade 03"

The following steps show how this can be set up in FAW:

1) Setup custom security assignment data in custom schema

- Login to ADW's custom schema (OAX$OAC).
- Create a table as per the custom security Assignments requirement per user.
  - For this use case, create a custom table with following columns
    - USERNAME

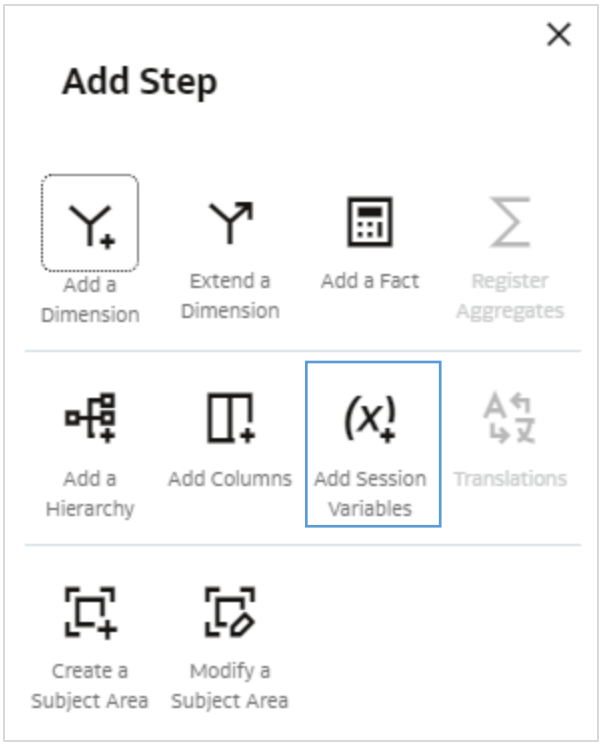
- SEC_OBJ_CODE
- SEC_OBJ_NUMBER
- SEC_OBJ_NAME

- As an analyst and line manager Ravi has access to multiple departments and grades, so insert one record for each of those.

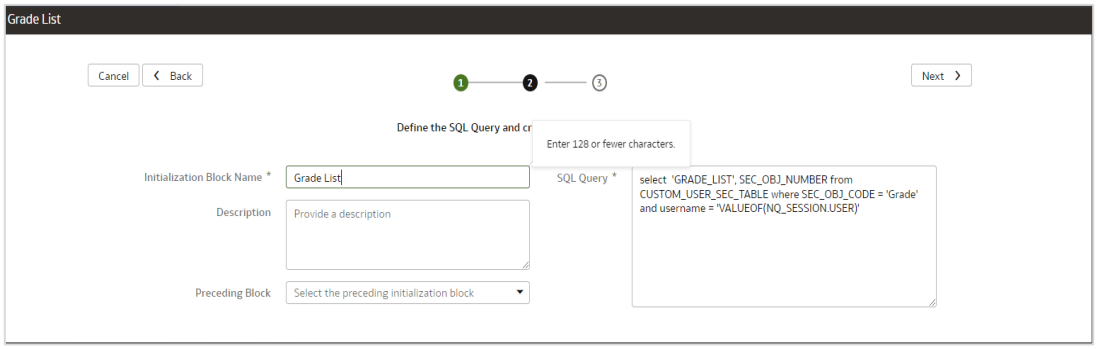
	USERNAME	SEC_OBJ_CODE	SEC_OBJ_NUMBER	SEC_OBJ_NAME
1	TM-RCHOUHAN	Department	3838	DP800 - Diretoria de Projetos
2	TM-RCHOUHAN	Department	281	Human Resources-East
3	TM-RCHOUHAN	Department	279	Human Resources-West
4	TM-RCHOUHAN	Department	226	Maintenance-South
5	TM-RCHOUHAN	Department	218	Production Control-Plant 4
6	TM-RCHOUHAN	Department	210	Seattle Distribution Center
7	TM-RCHOUHAN	Department	708	US Sales East
8	TM-RCHOUHAN	Department	202	Vision Corporation Enterprise
9	TM-RCHOUHAN	Department	300100150014361	Engineering
10	TM-RCHOUHAN	Department	1000000154600 65	BI_HR-Dept14-Business Visit Unit
11	TM-RCHOUHAN	Grade	100000015162133	BI_HR_M2 - Manager Pay Grade 02
12	TM-RCHOUHAN	Grade	100000015162072	BI_HR_IC3 - Individual Contributor Pay Grade 03
13	TM-RCHOUHAN	Grade	25	200.2.East
14	TM-RCHOUHAN	Grade	23	200.2.West
15	TM-RCHOUHAN	Grade	100000011571150	IT4
16	TM-RCHOUHAN	Grade	100000011571146	IT3
17	TM-RCHOUHAN	Grade	100000015162128	BI_HR_M1 - Manager Pay Grade 01
18	TM-RCHOUHAN	Grade	100000000000017	IC4
19	TM-RCHOUHAN	Grade	100000000000018	IC5
20	TM-RCHOUHAN	Grade	100000000000021	M-3
21	TM-RCHOUHAN	Grade	100000011571154	IT5

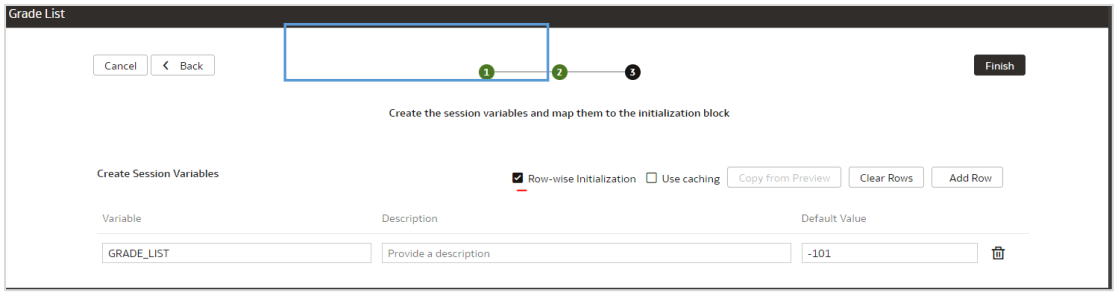
2) Customize FAW to create session variables to return list of departments, grades for logged in user

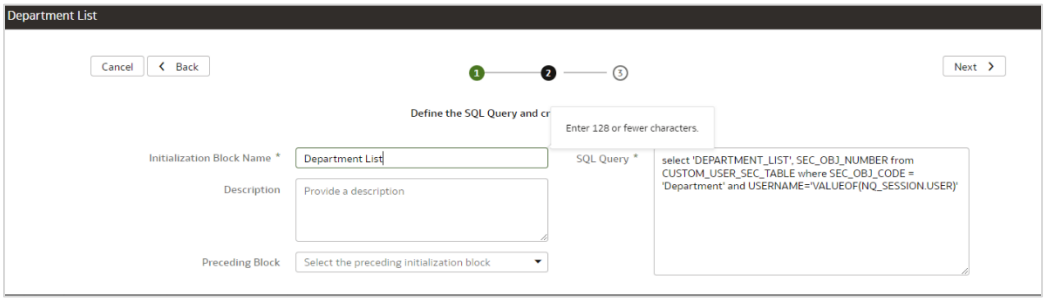
- Log in to the FAW console as a Service Admin (or a user assigned a modeler role)
- Navigate to Semantic **Model Extensions User Extensions**
- Create a **Branch** and **Add Step → Add Session Variables**

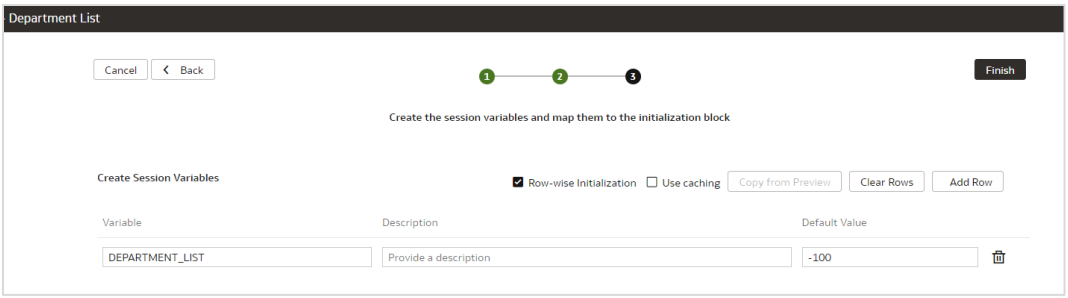


- Add Session variables for grade and department list. You will also need to create the Initialization blocks as part of the process. Ensure the "**Row-wise initialization"** check box is selected if the variable is to return a list of values

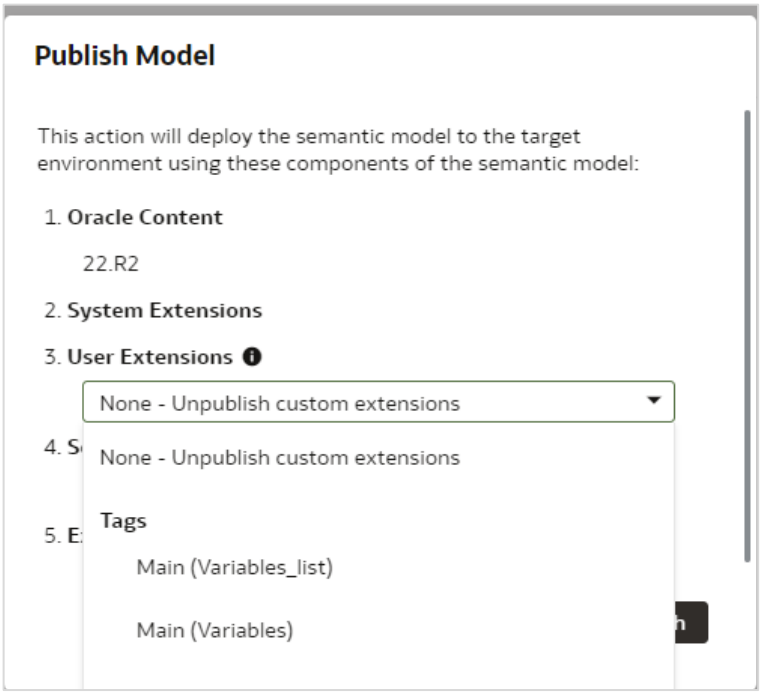






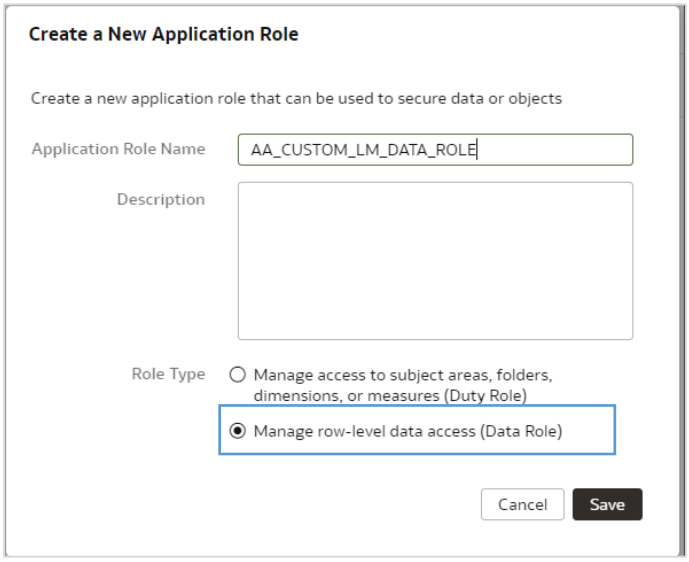


- **Merge** the steps to Main branch
- Click **Create a Tag** and name it appropriately, e.g., Variable_List
- **Publish Model**

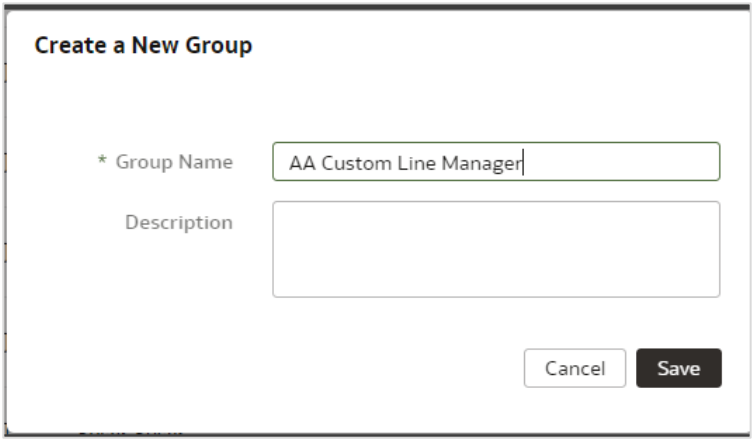


3) Create Custom Roles in the Security Console

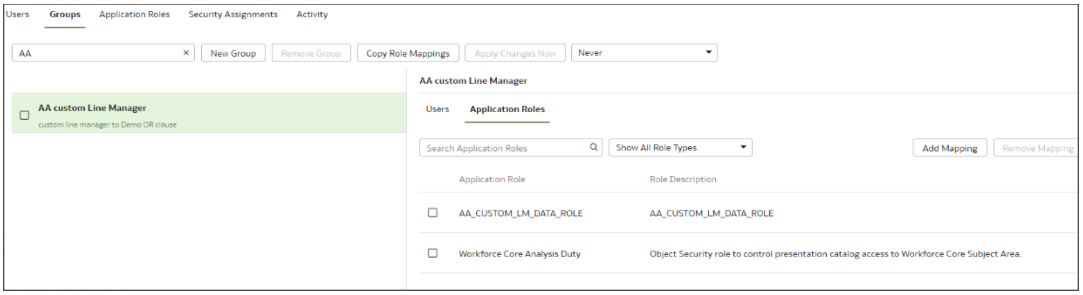
- Navigate to **Console → Security Application Roles**
- Create new Application role: AA_CUSTOM_LM_DATA_ROLE



- Navigate to **Security → Groups**
- Create new Group**:** AA Custom Line Manager



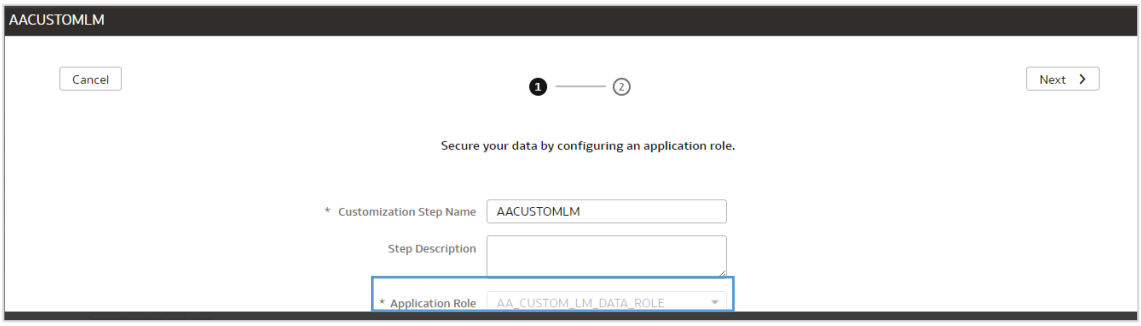
- Add **AA_CUSTOM_LM_DATA_ROLE** to **AA Custom Line Manager** Group
- Add Required Duty roles



- Add user TM-RCHOUHAN (Ravi Chouhan) to the group

4) Setup data filters for the custom role

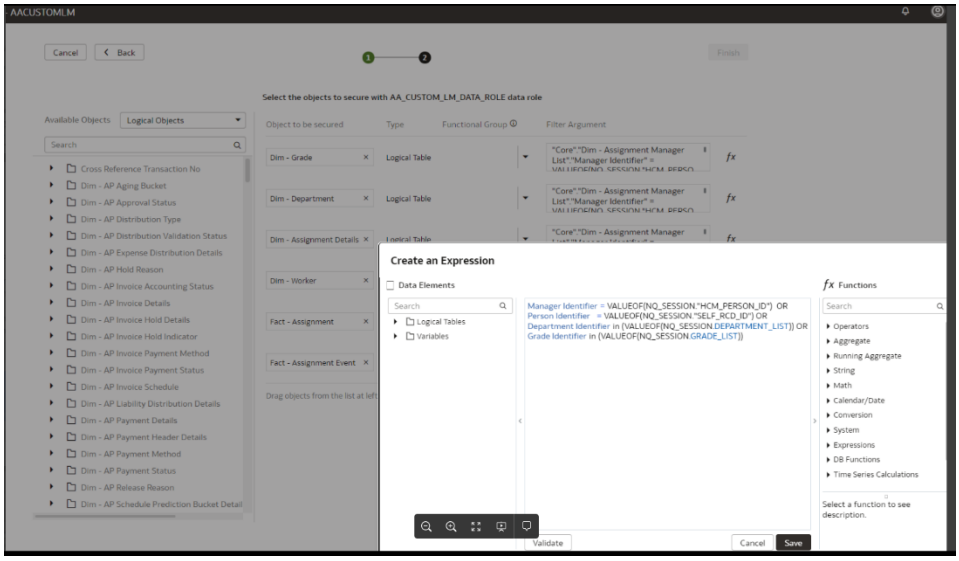
- Navigate to **Console → Semantic Model Extensions Security Configurations**
- Click Add **Data Security Step**
  - Provide a step name
  - Choose **AA_CUSTOM_LM_DATA_ROLE** for the application role. Click Next



  - Choose Logical Objects from the Available Objects dropdown and add security clause for each object to be secured.
  - Sample:

```
"Core"."Dim - Assignment Manager List"."Manager Identifier" = VALUEOF(NQ_SESSION."HCM_PERSON_ID") OR
"Core"."Dim - Worker"."Person Identifier" = VALUEOF(NQ_SESSION."SELF_RCD_ID") OR
"Core"."Dim - Department"."Department Identifier" IN (VALUEOF(NQ_SESSION.DEPARTMENT_LIST)) OR
"Core"."Dim - Grade"."Grade Identifier" IN (VALUEOF(NQ_SESSION.GRADE_LIST))
```

    - Dim – Grade
    - Dim – Department
    - Dim – Assignment Details
    - Dim – Worker
    - Fact – Assignment
    - Fact – Assignment Event



- Click **Finish**
- **Publish** Model
- Monitor the published activity, until it is completed.

Examine the Physical SQL generated for Ravi Chouhan

In the generated Physical SQL, you would notice that there is an OR clause generated with the contexts used in security:

```
AND (T240.MANAGER_ID                IN (100000008153757.0)
OR T586.GRADE_ID                    IN (23.0, 25.0, 100000000000017.0, 100000000000018.0, 100000000000021.0, 100000011571146.0, 100000011571150
OR T1039.PERSON_ID                  IN (100000008153757.0)
OR T1826.DEPARTMENT_ID              IN (202.0, 210.0, 218.0, 226.0, 279.0, 281.0, 708.0, 3838.0, 100000015460065.0, 300100150014361.0))
```

Points to note

While implementing custom data security, the following points should be noted:

1. Do not re-use any data roles delivered out-of-the-box (OOTB) in FAW. The behavior of these seeded roles cannot be altered if used as part of a custom role implementation. This includes using functional group construct on OOTB roles – this is not supported.
2. All data roles used as part of a custom security implementation need to be custom roles
3. Create a custom role for each unique combination of dimension security context. For example, if you need to configure data security for a group of users by Line Manager + Department + Grade, and another group by Line Manager + Grade, create separate data roles for each
4. Create a custom role for each variation of AND vs OR scenario, even though the same combination of dimension is to be used. For example, if a Line Manager needs to have data secured by Line Manager OR (Business Unit AND Grade), and the HR analyst role also needs the same, they are two different personas having different security. You will need to create a separate custom role for each such scenario.

5. Secure all required facts and dimensions with these custom roles. You should not combine facts and dimensions that are partially secured by these custom roles, i.e., some are secured by custom roles while others are secured by out-of-the-box roles. Custom and out-of-the-box roles cannot be applied together.

Conclusion

The FAW security framework provides robust capabilities to secure user access to analytic objects and the data shown within those objects. The framework also allows you to implement your own security rules, as shown in the sections above. It should be kept in mind that implementing custom security is often complex and requires a good understanding of your business rules, the tools and options available to customize security and availability of technical and functional resources. We encourage customers considering implementation of this framework to consult with Oracle Partners and/or System Integrators, who bring considerable domain and technical knowledge to design, implement, automate and support complex, custom security implementations within FAW.