

**Liberty Health**

**Authentication/Roles**

**Project: Commissions Self-Build**

Prepared by: Jaco Bosman

LIFE INVESTMENTS HEALTH CORPORATE PROPERTIES ADVICE

DOCUMENT HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Status | Amended by | Changes |
| 1.0 | 01-04-2018 | Draft | Jaco Bosman |  |

TABLE OF CONTENTS

Contents

[Purpose 2](#_Toc511133483)

[1. Roles 2](#_Toc511133484)

[2. Authentication 7](#_Toc511133485)

# Purpose

The purpose of this document is to illustrate the ADF roles and authentication architecture Home Application

# Roles

The roles access is always granted on the lowest required level in the ADF system.

* 1. Application Roles

The application roles are what is assigned to the functions within the ADF system and is what gets used to limit functions to users. There are 5 application roles within the system:

* Viewer - Can view but action nothing
* BDM Consultant - Can create/maintain Brokers and Brokerages
* Commissions Consultant - Can do most functions except approve runs/payments
* Team Lead - Can do all operational functions
* Super User - Can add and maintain administration tables and system parameters
  1. Enterprise roles

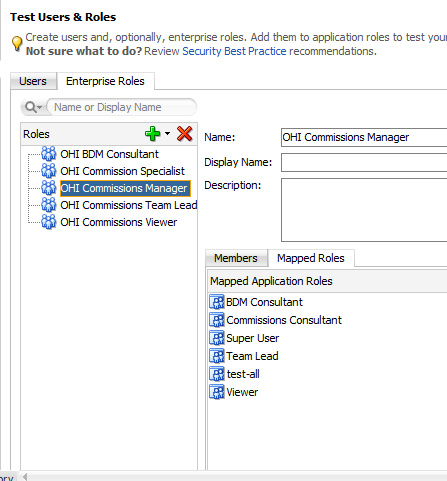
There are 5 enterprise roles for the commission system. These enterprise roles have the exact same name on Active Directory and get linked via the Weblogic server. The enterprises roles are then assigned the necessary application roles, explained in 1.1.

The enterprise roles are:

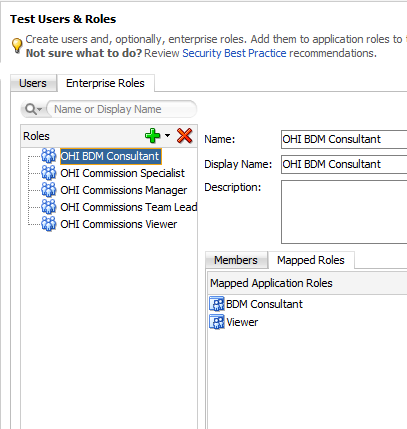
* OHI Commissions Viewer
* OHI BDM Consultant
* OHI Commission Specialist
* OHI Commissions Team Lead
* OHI Commissions Manager

An enterprise role can be assigned to one or more application roles. Taking the example of the OHI Commissions Manager.

As depicted below the OHI Commissions Manager enterprise role has been granted ALL of the application roles, as the manager should have all access on the system.



Looking at the BDM Consultant role, which should only limited access, only the BDM consultant and viewer application roles were granted.



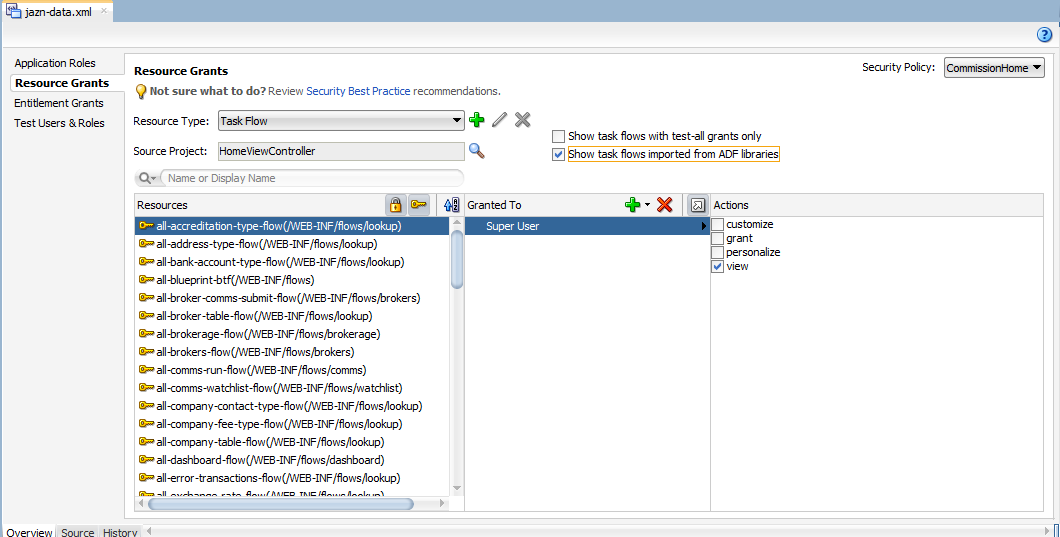
This configuration allows the application to control what each role has access to what, without constantly changing/modifying the enterprise or active directory configuration.

* 1. Granting application roles access

The role configuration is stored in the jazn-data.xml file. This file is only available from the Commission Home application.

To access the configuration:

* Open Commissions Home application
* Click the Application menu item
* Select the Secure sub menu item
* Select Resource Grants

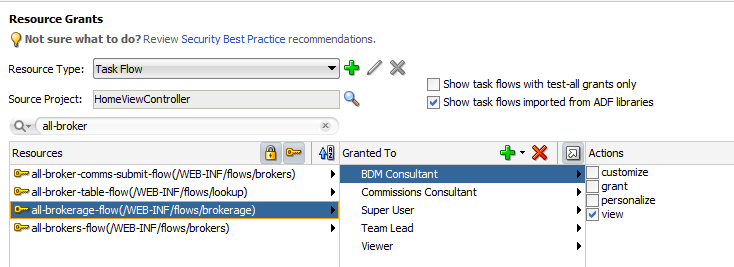


* Ensure you tick the "Show task flows imported from ADF Libraries" checkbox

The Resource Grants screen is where you link the task-flows to the application role level of user access required to action that screen/flow.

In the above example, the all-accreditiation-type-flow has only been granted the Super User application role, as this is a very restrictive function.

In the below example, we're looking at the all-brokerage-flow. This screen/flow should be available to all users, even the viewer. Therefore we have granted all the application roles.

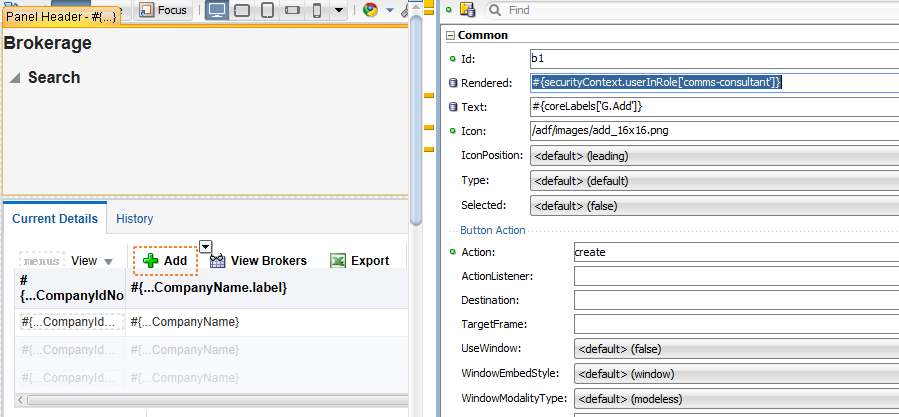


* Access needs to be granted to all flows, this means flows from the BTF project as well as the flows from the view controller application. If the user doesn't have access to the flow and the screen navigates to the flow, the user will be told they don't have access.
  1. Limiting functions in application

Some of the buttons or navigation in the application needs to be visible or able for certain roles. In order to achieve this, you set the visible or rendered property of the object (button/table/export button etc) with the lowest role access required:

#{authenticationContext.userInRole[*'role\_name'*]}

This expression will return true or false and will then set the rendered or visible property to the same value, thus either showing the user the function or not



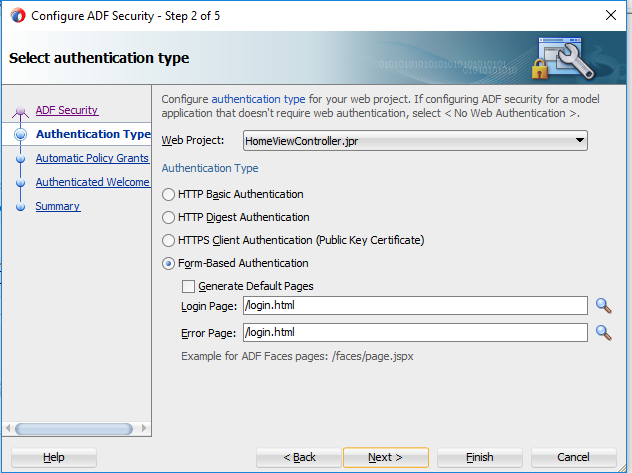
# Authentication

2.1 Authentication Type

The application authentication is controlled by a login page. The login page can be found in the Commission Home application.

The configuration for which type of authentication the application uses can be done by:

* Open Commissions Home application
* Click the Application menu item
* Select the Secure sub menu item
* Select Configure



Implementing SSO would require the configuration to be changed from Form-Based to http basic auth.

2.2 Granting user authentication

Users are granted access by assigning the user to one of the application roles in Active Directory. This has to be done by Alfonso's team. The team lead/manager needs to log a request for them to action this. Once the user has been assigned to that role in AD, the user can log into the application using their windows logon cridentials.