

Oracle Financial Services Capital Adequacy Pack Admin Guide

Release 8.0.6.0.0

May 2018



TABLE OF CONTENTS

1	ABOUT OFS CAPITAL ADEQUACY APPLICATION PACK RELEASE 8.0.6	1
2	OFS BASEL REGULATORY CAPITAL IRB AND BASIC	2
2.1	Introduction	2
2.2	Role of an Administrator	2
2.3	Function Maintenance	3
2.4	Function Maintenance	6
2.5	Role Maintenance	9
2.6	Function - Role Mapping for Basel UI	12
2.7	User Group Role Map	15
2.8	Performance Tuning	16
3	OFS BASEL REGULATORY CAPITAL ANALYTICS CONFIGURATION	18
3.1	Introduction	18
3.1.1	Assumptions	18
3.1.2	Prerequisites	18
3.2	Configuration Steps	18
3.2.1	Script Execution	18
3.2.2	Server Configuration Steps	19
3.2.3	Application Roles	23
3.2.4	Dashboard/Answer Reports (from any client machine or Windows machine)	24
3.2.5	Dashboard Report Verification	27
3.2.6	Installation of Images (Only for New Installation):	30
3.2.7	BI Publisher Reports (Only for New Installation):	30
3.3	Post configuration verification steps	32
3.4	Configuring OBIEE link in OFSAAI Framework	33
3.5	Oracle Financial Services Electronic Submission Administration Activities	33
3.6	User Administrator	34
3.6.1	User Maintenance	34
3.6.2	UserGroup Maintenance	38
3.6.3	User UserGroup Map	41
3.6.4	Profile Maintenance	42
3.6.5	User Authorization	44
3.6.6	User Group Authorization	45
3.6.7	UserGroup Domain Map	46

3.6.8	UserGroup Role Map	47
3.7	System Administrator	52
3.7.1	Assumptions	52
3.7.2	Pre-Requisites	53
3.7.3	Installing and Configuring SMTP on Web Application Server.....	53
3.7.4	Creating a New Access Control List	54
3.7.5	Access of Web Application Server to SMTP server	56
3.7.6	Data Preparation for Mail Utility	56
3.7.7	SETUP DATA	72
3.7.8	MASKING DATA PREPARATION.....	75
4	OFS ECONOMIC CAPITAL ADVANCED ANALYTICS CONFIGURATION.....	79
4.1	Assumptions.....	79
4.2	Prerequisites	79
4.3	Configuration Steps.....	80
4.3.1	Server Configuration Steps	80
4.3.2	Dashboard/Answer Reports	83
4.3.3	Installation of Images (Only for New Installation)	84
4.3.4	Post Configuration Verification Steps	85
5	OFS OPERATIONAL RISK ECONOMIC CAPITAL ANALYTICS CONFIGURATION.....	86
5.1	Assumptions.....	86
5.2	Prerequisites	86
5.3	Configuration Steps.....	87
5.3.1	Server Configuration Steps	87
5.3.2	Dashboard/Answer Reports	90
6	DATA PRIVACY FEATURES IMPLEMENTATION BY OFSAA.....	91
6.1	Data Redaction	91
6.1.1	Prerequisites	91
6.1.2	Executing Data Redaction Utility	92
6.2	Right to be Forgotten	95
6.2.1	Prerequisites	95
6.2.2	Executing Right to be Forgotten Utility.....	95
6.3	Data Privacy for OBIEE.....	98
6.3.1	Prerequisites	98
6.3.2	Executing OBIEE Utility.....	99

1 About OFS Capital Adequacy Application Pack Release 8.0.6

OFS Capital Adequacy Pack Release 8.0.6 includes the following applications:

- **Oracle Financial Services Economic Capital Advanced:** This application provides integrated risk and capital management solution with built-in statistical modeling features for advanced risk analytics and decision support systems.
- **Oracle Financial Services Basel Regulatory Capital Basic:** The application encompasses Credit, Market, and Operational Risks and provides a detailed breakup of the Capital Requirements across Tier 1, 2 and 3. The application supports the computation of Capital Adequacy Ratio (CAR) as per the guidelines laid out in the BIS (Basel I, Basel II and Basel III), India, USA, Islamic Banking, Brazilian, and CBRC jurisdictions.
- **Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach:** This application is based on the approaches supported by the OFS Basel Regulatory Capital Basic Application as well as the advanced approaches for BIS, USA, and CBRC Jurisdictions.
- **Oracle Financial Services Basel Regulatory Capital Analytics:** This application allows institutions to capitalize on their Basel II compliance investments by providing extensive dashboards that enable efficient and timely Pillar I analysis and Pillar 3 disclosures, regulatory reporting and provide a complete platform for strategic decision-making across the institution.
- **Oracle Financial Services Operational Risk Economic Capital:** This application provides pre-configured models based on actuarial methods that enable institutions to calculate capital for operational risk. This is achieved through the computation of the risk measures such as Operational Risk VaR and Conditional VaR.
- **Oracle Financial Services Retail Portfolio Risk Models and Pooling:** This application, which is a part of the Oracle Financial Services Enterprise Risk Management suite of advanced risk analytical applications, provides a pre-built, scalable and easily deployable method for retail pooling and loss measure estimation.

2 OFS Basel Regulatory Capital IRB and Basic

2.1 Introduction

Compliance to the Basel accord is a mandated business requirement for financial institutions in most jurisdictions around the world. Financial institutions need a complete solution that allow them to quickly respond to these requirements and provides them with an in-depth analysis of regulatory capital requirements under baseline and stress scenarios for effective capital planning. With the latest Oracle Financial Services Basel Regulatory Capital application, banks can now meet requirements as mentioned in the Basel accord, in multiple jurisdictions with a single application, thereby eliminating the need for multiple point applications from multiple software vendors. The application encompasses Credit, Market, and Operational Risks and provides a detailed breakup of the Capital Requirements across Tier 1, 2 and 3. The application supports the computation of Capital Adequacy Ratio (CAR) as per the guidelines laid out in the BIS (Basel I, Basel II and Basel III), India, USA, Islamic Banking, Brazilian, and CBRC jurisdictions.

2.2 Role of an Administrator

There are two types of Administrators as defined by the OFS Analytical Applications Infrastructure: A User Administrator and System Administrator.

System Administration: refers to a process of managing, configuring, and maintaining confidential data in a multi-user computing environment. A System Administrator in creates functions, roles, and mapping functions to specific roles. A System Administrator also maintains segment information, holiday list, and restricted passwords to ensure security within the application.

User Administration: is one of the core functions of Security Management which involves administrators to create user definitions, user groups, maintain profiles, authorize users and usergroups, and map users to groups, domains and roles. A User Administrator controls the user privileges in accessing the application and is based on business requirements to provide access to view, create, edit, or delete confidential data.

A User Administrator grants permissions based on user roles and requirements. The function roles SYSADM and METAAUTH function roles should be mapped, to access User Administrator in LHS menu of Security Management. The following sections detail the following activities of a System Administrator and User Administrator:

System Administrator:

- Function Maintenance
- Role Maintenance
- Function-Role Mapping

User Administrator:

- User Group Role Map

2.3 Function Maintenance

Overview

A function defines the privileges to access modules or components in the OFS Basel Regulatory Capital Application and, defines or modifies associated metadata information. Function maintenance allows you to create functions for users to ensure only those functions are executed which are specific to the user's role. To access Function Maintenance:

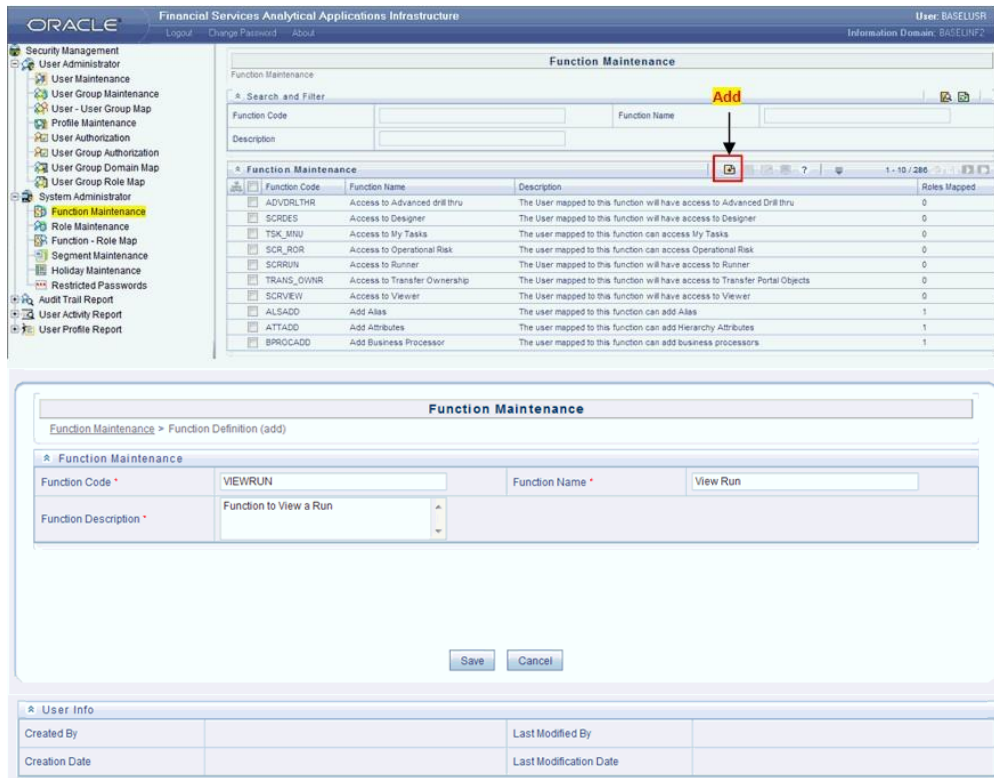
1. Expand the Administration menu in the LHS menu of the OFSAAI.
2. Click Security Management.
3. Expand the System Administrator menu in the LHS menu of the OFSAAI.
4. Click Function Maintenance.

The Function Maintenance screen displays the function details such as Function Code, Function Name, Description and the number of Roles Mapped to the function. The Function Maintenance screen also facilitates you to view, create, modify, and delete functions within the system. You can also make use of Search and Pagination options to search for a specific function or view the list of existing functions within the system.

Create Function

To create function in the Function Maintenance screen:

1. Select **Add** icon from the Function Maintenance tool bar. Add icon is disabled if you have selected any function in the grid. The New Function screen is displayed.



2. Enter the function details as tabulated.

Field	Description
Function Code	Enter a unique function code. Ensure that there are no special characters and extra spaces in the code entered. For example, VIEWRUN to view a Run.
Function Name	Enter a unique name for the function. Ensure that the Function Name does not contain any special characters except "(,)", "_", "-", "."
Function Description	Enter the function description. Ensure that the Function Description does not contain any special characters except "(,)", "_", "-", "."

Note: Fields marked with an "*" are mandatory fields and must be updated.

3. Click **Save** to upload the function details.

The User Info grid at the bottom of Function Maintenance screen displays metadata information about the function created.

View Function

You can view individual function details at any given point. To view the existing user details in the Function Maintenance screen:

1. Select the checkbox adjacent to the Function Code.
2. Click **View** icon in the Function Maintenance tool bar.



The View Function Details screen is displayed with the details such as Function Code, Function Name, and Function Description.

Modify Function

To update the existing function details (other than system generated functions) in the Function Maintenance screen:

1. Select the checkbox adjacent to the required Function Code.
2. Click **Edit** Icon in the Function Maintenance tool bar. The Edit Function Details screen is displayed.



3. Update the required information.

Note: Function Code cannot be edited.

4. Click **Save** to upload the changes.

Delete Function

You can remove only those function(s) created by you and which are no longer required in the system, by deleting from the Function Maintenance screen.

1. Select the checkbox adjacent to the Function Code whose details are to be removed.



2. Click **Delete** icon in the Function Maintenance tool bar.
3. Click **OK** in the information dialog to confirm deletion.

2.4 Function Maintenance

Overview

A function defines the privileges to access modules or components in the OFS Basel Regulatory Capital Application and, defines or modifies associated metadata information. Function maintenance allows you to create functions for users to ensure only those functions are executed which are specific to the user's role. To access Function Maintenance:

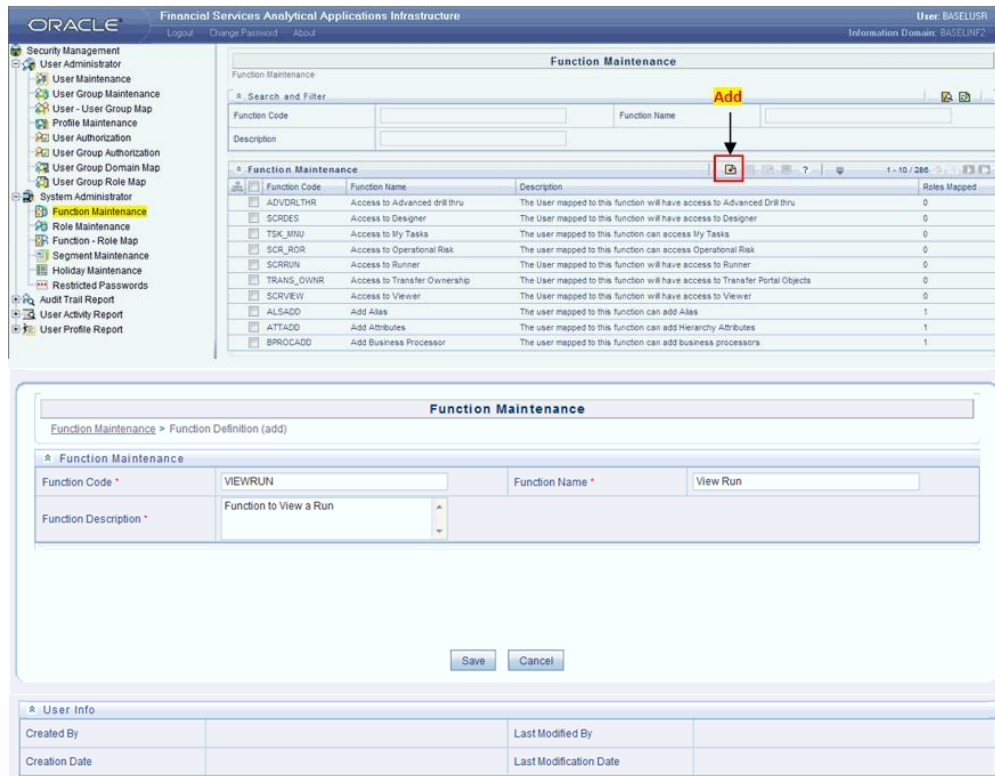
1. Expand the Administration menu in the LHS menu of the OFSAAI.
2. Click Security Management.
3. Expand the System Administrator menu in the LHS menu of the OFSAAI.
4. Click Function Maintenance.

The Function Maintenance screen displays the function details such as Function Code, Function Name, Description and the number of Roles Mapped to the function. The Function Maintenance screen also facilitates you to view, create, modify, and delete functions within the system. You can also make use of Search and Pagination options to search for a specific function or view the list of existing functions within the system.

Create Function

To create function in the Function Maintenance screen:

1. Select **Add** icon from the Function Maintenance tool bar. Add icon is disabled if you have selected any function in the grid. The New Function screen is displayed.



2. Enter the function details as tabulated.

Field	Description
Function Code	Enter a unique function code. Ensure that there are no special characters and extra spaces in the code entered. For example, VIEWRUN to view a Run.
Function Name	Enter a unique name for the function. Ensure that the Function Name does not contain any special characters except "(", ")", "_", "-", "."
Function Description	Enter the function description. Ensure that the Function Description does not contain any special characters except "(", ")", "_", "-", "."

Note: Fields marked with an "*" are mandatory fields and must be updated.

3. Click **Save** to upload the function details.

The User Info grid at the bottom of Function Maintenance screen displays metadata information about the function created.

View Function

You can view individual function details at any given point. To view the existing user details in the Function Maintenance screen:

1. Select the checkbox adjacent to the Function Code.
2. Click **View** icon in the Function Maintenance tool bar.



The View Function Details screen is displayed with the details such as Function Code, Function Name, and Function Description.

Modify Function

To update the existing function details (other than system generated functions) in the Function Maintenance screen:

1. Select the checkbox adjacent to the required Function Code.
2. Click **Edit** Icon in the Function Maintenance tool bar. The Edit Function Details screen is displayed.



3. Update the required information.
- Note:** Function Code cannot be edited.
4. Click **Save** to upload the changes.

Delete Function

You can remove only those function(s) created by you and which are no longer required in the system, by deleting from the Function Maintenance screen.

1. Select the checkbox adjacent to the Function Code whose details are to be removed.
2. Click **Delete** icon in the Function Maintenance tool bar.



3. Click **OK** in the information dialog to confirm deletion.

2.5 Role Maintenance

Overview

A role is a collection of functions defined for a set of users to execute a specific task. You can create roles based on the group of functions to which users are mapped. To access Role Maintenance:

1. Expand the Administration menu in the LHS menu of the OFSAAI.
2. Click Security Management.
3. Expand the System Administrator menu in the LHS menu of the OFSAAI.
4. Click Role Maintenance.

The Role Maintenance screen displays the role details such as Role Code, Role Name, Role Description and the number of Users Mapped to the role. The Role Maintenance screen also facilitates you to view, create, modify, and delete roles within the system. You can also make use of Search and Pagination options to search for a specific role or view the list of existing roles within the system.

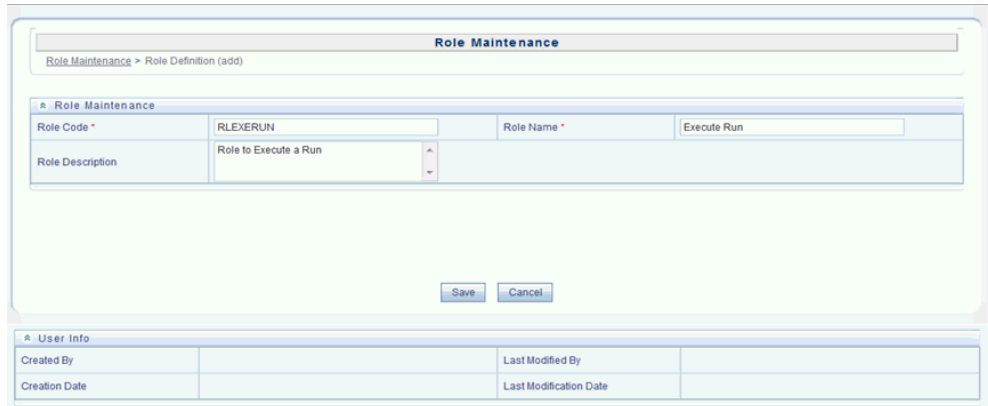
The default codes defined in the application are as follows:

Role Code	Role Description
GLDROLE	Role to access Run Management
RLEXERUN	Role to execute a Run
RLMODPRM	Role to modify Run Parameters
RLVIEWRUN	Role to view Run Details
ATTROLE	Role to access to Attribution link
RUN ROLE	Role to access Run Definition link

Create Role

To create a role in the Role Maintenance screen:

1. Click **Add** icon from the Role Maintenance tool bar. Add icon is disabled if you have selected any role in the grid. The New Role screen is displayed.



2. Enter the role details as tabulated.

Field	Description
Role Code	Enter a unique role code. Ensure that there are no special characters and extra spaces in the code entered. For example, ACTASR to create Action Assessor.
Role Name	Enter a unique name for the role. Ensure that the Role Name does not contain any special characters except space.
Role Description	Enter the role description. Ensure that the Role Description does not contain any special characters except space.

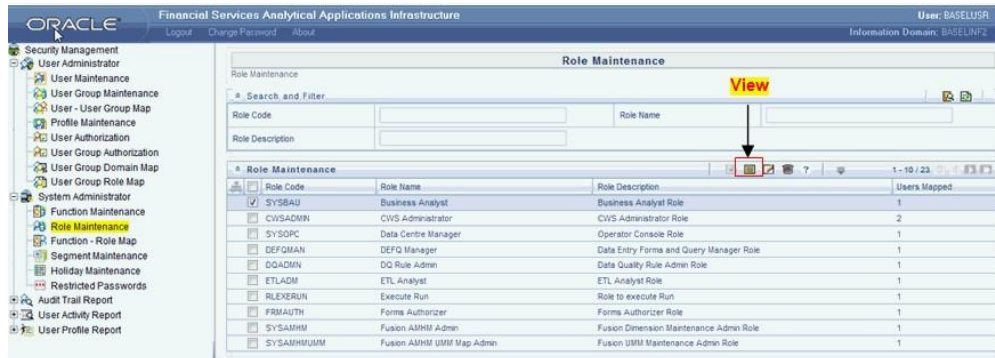
3. Click **Save** to upload the role details.

The User Info grid at the bottom of Role Maintenance screen display metadata information about the role created.

View Role

You can view individual role details at any given point. To view the existing role details in the Role Maintenance screen:

1. Select the checkbox adjacent to the Role Code.
2. Click **View** icon in the Role Maintenance tool bar.



The View Role Details screen is displayed with the details such as Role Code, Role Name, and Role Description.

Modify Role

To update the existing role details in the Role Maintenance screen:

1. Select the checkbox adjacent to the required Role Code.
2. Click **Edit** icon in the Role Maintenance tool bar. The Edit Role Details screen is displayed.



3. Update the required information.

Note: Role Code and Role Name cannot be edited.

4. Click **Save** to upload the changes.

Delete Role

You can remove only those role(s) which are created by you, which does not have any users mapped, and which are no longer required in the system by deleting from the Role Maintenance screen.

1. Select the checkbox adjacent to the Role Code whose details are to be removed.
2. Click **Delete** icon in the Role Maintenance tool bar.



3. Click **OK** in the information dialog to confirm deletion.

2.6 Function - Role Mapping for Basel UI

Overview

Function Role Map facilitates you to view and map a set of function(s) to a specific role within the OFS Basel Regulatory Capital application. Functions can only be mapped to a defined set of roles to ensure effective system security. The system administrator can create new roles and assign the functions as required instead of using the default roles.

To access Function Role Map:

1. Expand the Administration menu in the LHS menu of the OFSAAI.
2. Click **Security Management**.
3. Expand the System Administrator menu in the LHS menu of the OFSAAI.
4. Click **Function-Role Map**.

The Function – Role Map screen displays a list of available Role Codes in alphabetical order with the Role Name. On selecting a particular Role Code, the Mapped Functions are listed in the Mapped Functions grid of Function – Role Map screen. The default Function – Role mapping defined within the application are as follows:

Roles	Function Mappings
Access Run Management	<ul style="list-style-type: none"> • BSLPORTADD (Function to add Portfolio Details) • BSLPORTVW (Function to View Portfolio Details) • BSLPORTEDT (Function to Edit Portfolio Details) • BSLPORTDEL (Function to Delete Portfolio)
Execute Run	<ul style="list-style-type: none"> • EXEREQRUN (Function to Execute the Requested Run) • MODRUNPRM (Function to Modify the Run Parameters) • VIEWRUNDET (Function to View the Run Details)
Modify Run Parameters	<ul style="list-style-type: none"> • MODRUNPRM (Function to Modify the Run Parameters)
View Run Details	<ul style="list-style-type: none"> • VIEWRUNDET (Function to View the Run Details)
Business Analyst	<ul style="list-style-type: none"> • POOLDEF (Function to view/add the Pooling definitions) • POOLDEL (Function to delete the Pooling definition) • OPTDEF (Function to view/add the Optimizer definitions) • OPTDEL (Function to delete the Pooling definitions) • FFIEC (The user mapped to this function can access FFIEC LINK)
Access Attribution link	<ul style="list-style-type: none"> • ATTFUNC (The user mapped to this function can access Attribution Link)
Access Run Definition Link	<ul style="list-style-type: none"> • RUNFUNC (The user mapped to this function can access Run definition link)

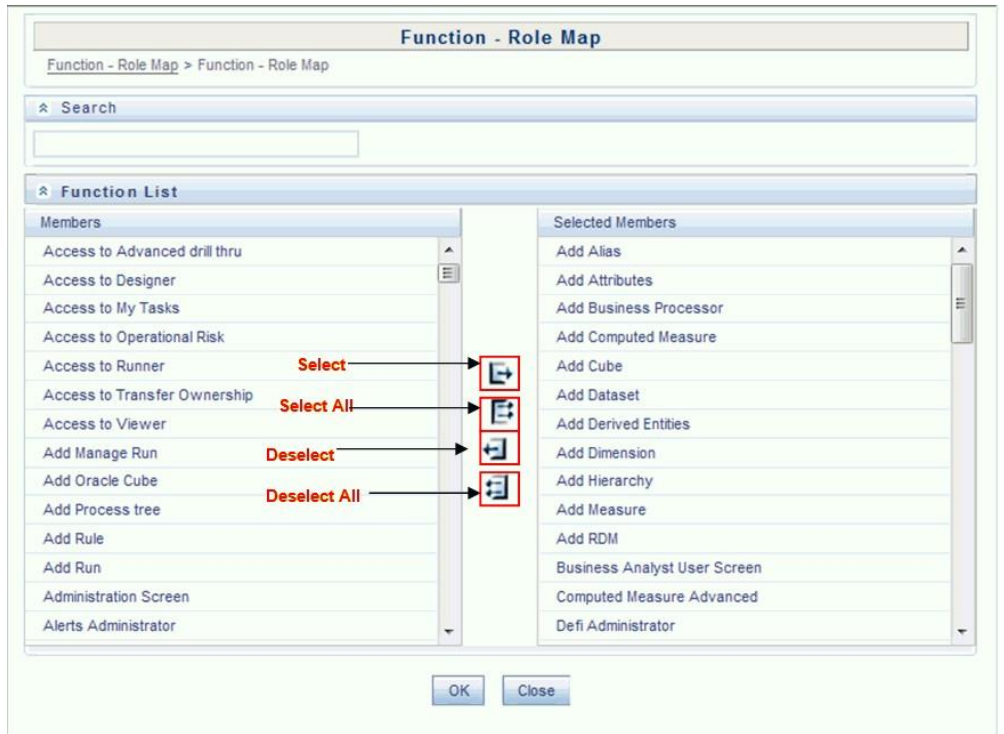
Mapping Function to a Role

To map a function to a role in the Function – Role Map screen, do the following:

1. Select the checkbox adjacent to the required Role Code. The Function – Role Map screen is refreshed to display the existing mapped functions.
2. Click **Edit** icon in the Mapped Functions section tool bar. The Function Role Mapping screen is displayed.



3. In the Function Role Mapping screen, you can search for a function using the Search field and edit the mapping.
 - To map a function to a role, select the function from the Members list and click **Select** icon. You can press **Ctrl** key for multiple selections.
 - To map all the functions to the selected role, click **Select All** icon.
 - To remove function mapping for a specific role, select the function from **Select Members** pane and click **Deselect** icon.
 - To remove all function mapping for a role, click **Deselect All** icon.



- Click **OK** to save the mappings and return to Function – Role Map screen.

2.7 User Group Role Map

Overview

User Group Role Map facilitates System Administrators to map Role(s) to specific User Group(s). Each role has a defined function and any user(s) mapped to the role has to perform only those functions. For example, the table below lists the user group mapped to a specific role.

GROUP CODE	ROLE CODE
ADMIN	SYSADM
AUTH	SYSATH
CWSADM	CWSADMIN

You can access User Group Role Map screen by expanding User Administrator section within the tree structure of LHS menu. The UserGroup Role Map screen displays a list of available user groups in alphabetical order with the User Group ID and Description. On selecting a user group, the list of available mapped roles are displayed. You can also make use of Search and Pagination options to search for specific usergroup or view the list of existing usergroups within the system.

Mapping Role to a User Group

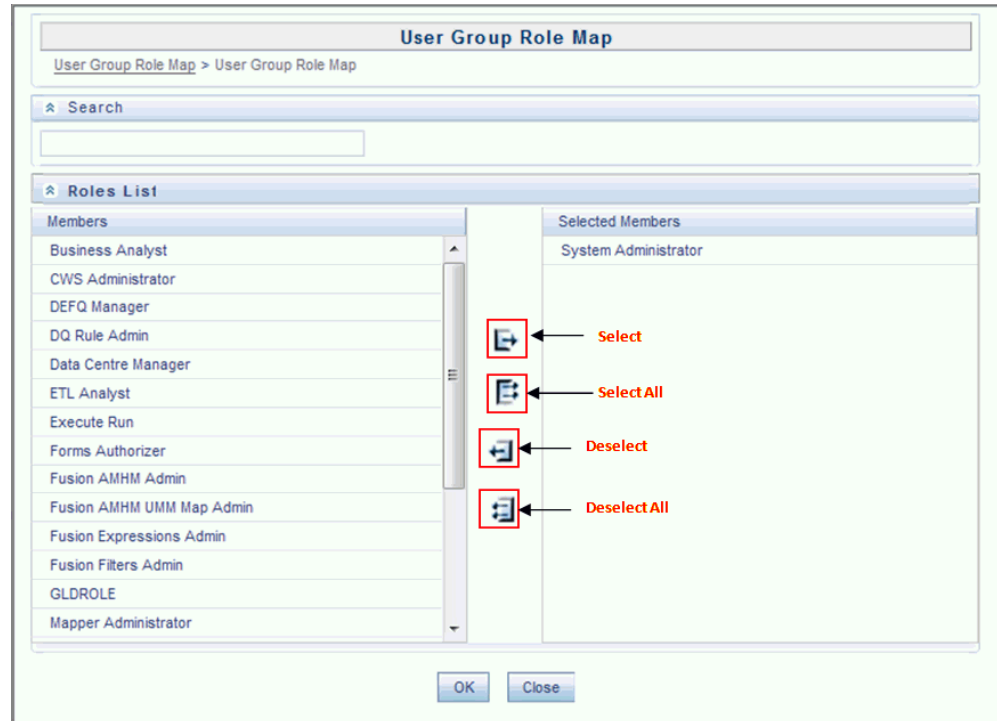
To map a Role to User Group, do the following:

- Select the checkbox adjacent to the required User Group ID. The User Group Role Map screen is refreshed to display the existing mapped roles.



- Click **Edit** icon in the Mapped Roles section tool bar. The User Group Role Map screen is displayed.
- In the User Group Role Map screen, you can search for a Role using the Search field and edit the mapping.

- To map Role to a User Group, select **Role** from the Members list and click the **Select** icon. You can press **Ctrl** key for multiple selections.
- To map all the Roles to a specific User Group, click **Select All** icon.
- To remove mapping for a user group, select **Role** from Select Members list and click the **Deselect** icon.
- To remove all Roles mapped to a User Group, click **Deselect All** icon.



4. Click **OK** to save the mappings and return to User Group Role Map screen.

2.8 Performance Tuning

Table Partitioning

The column `n_run_skey` is available in all the FACT tables of the OFS Basel Regulatory Capital application. This column stores a unique surrogate key for each Run execution. All records populated through a Run execution have the same value for `n_run_skey`.

Value of this column is incremented by one, for each execution. Hence, it is recommended to create interval partitions on the FACT tables with `n_run_skey` as the key of the partition. If Runs are executed in an immediate execution mode for different dates where `n_run_skey` remains the same across these dates, it is recommended to create range partition on the column `n_mis_date_skey`. It is also recommended to create a local index.

Parallel Executions

When you execute SQL statements in parallel, then multiple processes work simultaneously to execute a single SQL statement. To execute a statement faster than a single process, divide the work necessary to execute a statement among multiple processes. For more information to execute the T2Ts and Rules in parallel mode, refer to OFSAAI Administration Guide. To execute optimizer and pooling in parallel mode, uncomment the tag ALTER_STATEMENTS in Optimizer_Config.xml and Pooling_Config.xml respectively, which are available in ficdb/conf file. Appropriate degrees of parallelism must be set.

Result Cache

Result cache stores the results of SQL queries for re-use in subsequent executions. By caching the results of queries, you can avoid repetitions of time consuming and intensive operations that generates the result set in the first place (for example, sorting/aggregation, physical I/O, joins and so on). Result caching feature can be for queries as well functions. In OFS Basel Regulatory Capital application, there are functions for currency conversion, returning a parameter value for the given parameter code and so on. Many records exist that have the same input parameter values. Hence, result cache is implemented for these functions. Similarly, there are T2T expressions with sub-queries which fetch the same result set. Result cache is implemented for these as well.

Result cache is enabled in three ways: hint, alter session, or alter system. Default is MANUAL which indicates that we need to explicitly request caching via the RESULT_CACHE hint. However, it is recommended to enable the result cache using alter system so that hints need not to be provided time and again. The following command needs be executed by the DBA: ALTER SYSTEM SET RESULT_CACHE_MODE = FORCE.

3 OFS Basel Regulatory Capital Analytics Configuration

3.1 Introduction

3.1.1 Assumptions

- If Oracle Financial Services (OFS) Basel Regulatory Capital product is installed, then the table scripts need not be executed as described in [Section 3.2.1](#) of this document.
- The database schema will have proper privileges namely: **CONNECT**, **RESOURCE AND CREATE MATERIALIZED VIEW**, to execute the above mentioned scripts.
- OBIEE 11.1.1.7.150120 (64-bit) Server for the respective operating system is installed.
- Administrator knows how to start/shutdown the OBIEE servers namely;
 - Web logic Server
 - Oracle BI Server
 - Oracle BI Presentation Server
 - Oracle BI Java Host
- Administrator knows the OBIEE installation path.

3.1.2 Prerequisites

- a. Backup following OBIEE folders (*for existing installation, not required for new installation*) :
 - `<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIServerComponent\coreapplication_obis1\repository`
 - `<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog\<new folder created as part of Server Configuration steps>`
- b. Server details, that is, URL of OBIEE should be handy.
- c. Copy following files/folders from the release kit to the local machine:
 - `$FIC_HOME/CAP/catalog/`; this folder has the archive for dashboard (reports) and BIP related files. Do not unzip these files, as these files are not zip files.
 - `$FIC_HOME/CAP/repository/OFS Basel Regulatory Capital Analytics - Repository.zip`; this has the rpd file. Unzip this file on the local machine.
 - `$FIC_HOME/CAP/Images/OFS Basel Regulatory Capital Analytics - Images.zip`; this has image files which are used in the reports (for new installation). Unzip this file in the local machine.
 - `$FIC_HOME/CAP/dashboardconfiguration/CreateAppRoles.py`; this is a script which is used for application role creation (for new installation).

3.2 Configuration Steps

3.2.1 Script Execution

Execute the following attached scripts in the database, and in the order mentioned below.

- 5-ALTER_MATERIALIZED_VIEW_FOR_NOLOGGING_Script.sql (This script is provided to disable logging of materialized views, and the same can be used as per Bank's policy).



5-ALTER_MATERIALIZED_VIEW_FOR_NOLOGGING_Script.sql

- 6-REFRESH_MATERIALIZED_VIEW_Script.sql (This script is provided to refresh all the materialized views incase the data of the base tables have been modified or after loading of fresh data).

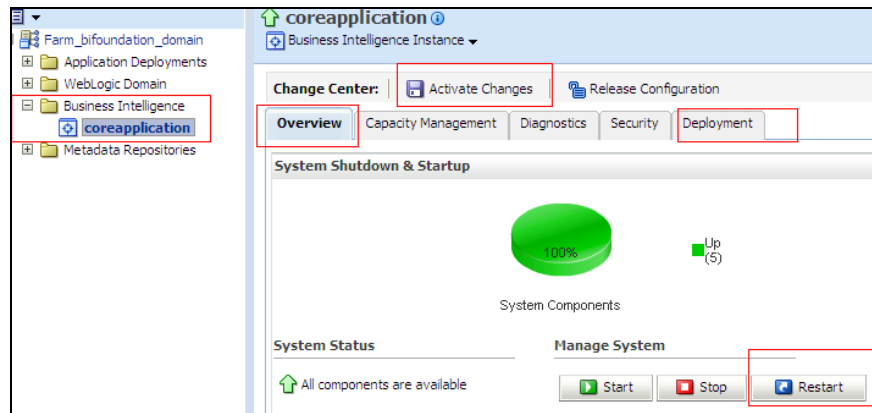


6-REFRESH_MATERIALIZED_VIEW_Script.sql

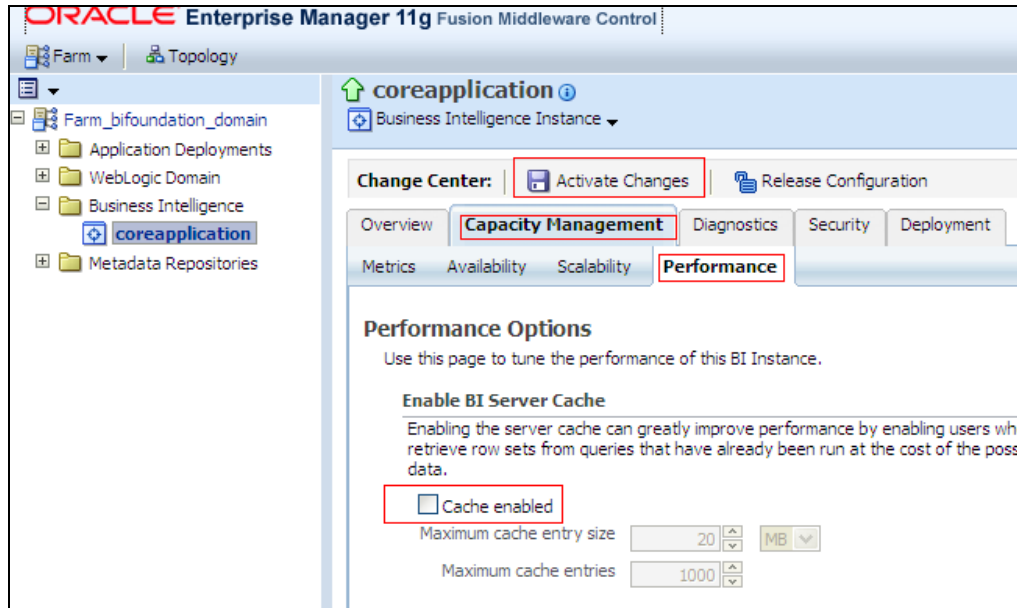
3.2.2 Server Configuration Steps

For each release, follow the below instructions for the server setup.

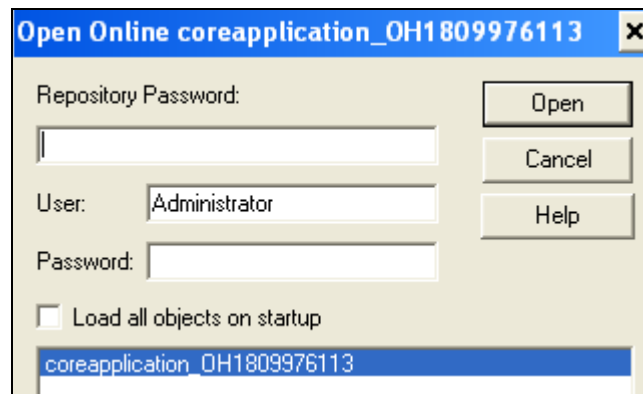
- Add the tnsnames.ora file in the following folder "*<Installation Path>middleware\Oracle_BI1\network\admin*". The **tnsnames.ora** file should contain the data-source connection details used in the connection pool of the RPD.
- Log on to Oracle Enterprise Manager.
 - Go to Business Intelligence menu located on the left hand side of the screen. Select **coreapplication** within it.
 - Go to **Deployment** located on the last tab.
 - Click **Lock and Edit** Configuration.
 - Go to the section Upload BI Repository.
 - Browse and select the repository.
 - Enter the repository password and confirm the same. The repository password is "Administrator1".
 - Go to BI Presentation Catalog section.
 - Edit the catalog path and remove SampleAppLite (Only in case of first time installation) from the end of the catalog path section and enter 'Basel' as the name of the new catalog folder. Make sure that the folder path is *<OBIEE Installation Path>middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog*
 - Click **Apply**.
 - Click **Activate Changes**.
 - Click **Overview** tab.
 - Click **Restart all**.



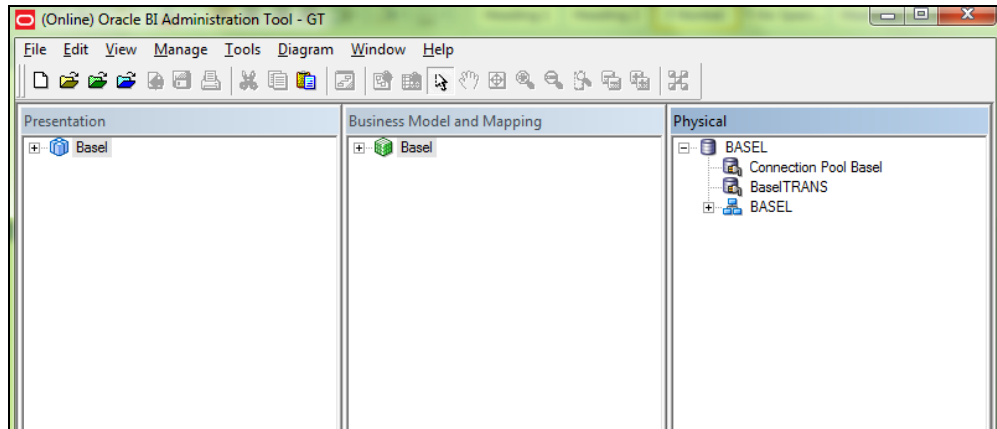
- xiii. Confirm to restart all opmn services.
- xiv. Edit the **NQSConfig.INI** file, found at *<Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1* to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = NO to YES.
- xv. Add the tag `<UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs>` in the **instanceconfig.xml** under the tag **<Catalog>**, found at *<Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent* and restart all opmn services.
- xvi. Check if all the servers are up and running (except Presentation Service).
- xvii. Edit the **NQSConfig.INI** file, found at *<Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1* to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES to NO.
Set EVALUATE_SUPPORT_LEVEL=2 from EVALUATE_SUPPORT_LEVEL=0 and save.
- xviii. Remove the tag `<UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs>` in the **instanceconfig.xml** under the tag **<Catalog>**, found at *<Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent*.
- xix. Restart all opmn services.
- xx. Disable the cache (cache can be enabled once the setup is moved to the production mode and on the basis of bank's requirements). To disable the cache, click on the "Capacity Management" tab in the Oracle Enterprise Manager. Select "Performance" tab within it. Click 'Lock and Edit Configuration' button. Un-check the option "Cache enabled". Click **Activate Changes**. Restart the servers to activate changes. Refer to the image below.



- c. Open the RPD online by clicking Start menu → All Programs → Oracle Business Intelligence → BI Administration



- d. Provide the Username and Password which have access to open RPD online and the Repository Password as **Administrator1**.
- e. Double click **Connection Pool Basel** in the physical layer of the RPD as shown in the figure below:

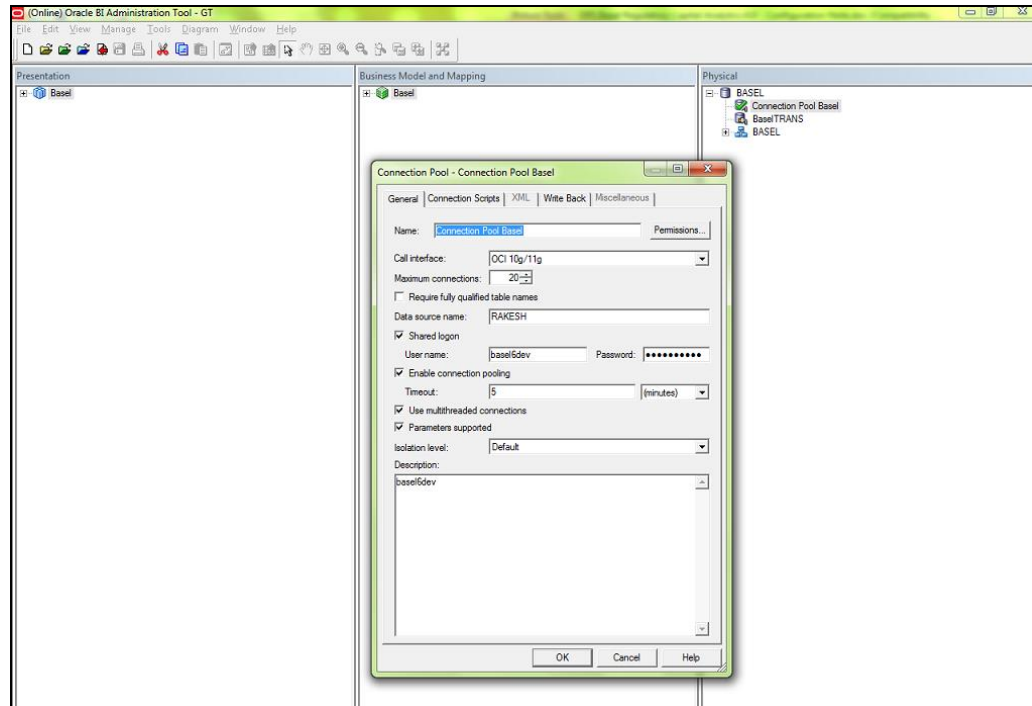
**Note:**

When the Oracle BI Server is running on Linux or UNIX and you need to update database object settings (such as the database type) or connection pool settings, you can copy the repository file to a Windows computer, make the changes using the Administration Tool on Windows, and then copy the repository file back to the Linux or UNIX computer.

- f. Change data source name, user name and password to the Oracle TNS Name, database schema name and password respectively, as shown in the diagram below.

Note:

If Oracle TNS Name is entered in Data Source Name, then TNS details must be also present under file - *<Installation Path>\Oracle_BI1\network\admin\tnsnames.ora*. Services must be restarted after addition of TNS details in the above mentioned path.



- g. Similarly, change the details for “BaselTRANS” (Database details where scripts SessionVariables_Create.sql and SessionVariables_Insert.sql are executed.)
- h. Save RPD and close it.
- i. Restart the opmn services.

3.2.3 Application Roles

- a. Open a command prompt and navigate to the folder “<OBIEE Installation Path>/oracle_common/common/bin/”.
- b. Execute the following command:

```
wlst <local file path>/CreateAppRoles.py <username> <password> t3://<obiee server's ipaddress>:<port no.>
```

Example: `wlst d:\BaselRoles\CreateAppRoles.py weblogic weblogic123 t3://10.184.202.205:7001`

3.2.4 Dashboard/Answer Reports (from any client machine or Windows machine)

- a. Start the BI services (if not started).
- b. Start OBIEE Catalog Manager (*Start* → *Programs* → *Oracle Business Intelligence* → *Catalog Manager*).
- c. Open Tools → *Preferences*.
- d. Check *Paste ACL* → *Create* and *Paste Overwrite* → *All*.
- e. Click **OK**.
- f. Select “*Open Catalog*” from File menu.
- g. Select the option “*Online*” for Type.
- h. Type the link for presentation services, that is, Oracle Interactive Dashboard link. For example (*http://URL:<port_number>/analytics/saw.dll?*).
- i. Give the Administrator user Id and password, and click OK.

Note:

Check [section 3.2.7](#) after un-archiving files for BI Publisher Reports (Only for New Installation).

1. Configuring Basel

- i. Click “*shared folder*” in the left hand pane.
- ii. Select the “*Un-archive option*” from File Menu and un-archive file “*OFS Basel Regulatory Capital Analytics - Basel_Dashboard*”, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create an “*Answers*” folder under “*shared folder*”.
- iv. Click “*Answers* folder” folder and un-archive file “*OFS Basel Regulatory Capital Analytics - Basel_Answers*”.
- v. Re-Start (stop and start) the BI services.

2. Configuring US

- i. Click “*shared folder*” in the left hand pane.
- ii. Select the “*Un-archive option*” from File Menu and un-archive file “*OFS Basel Regulatory Capital Analytics - US_Dashboard*”, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create an “*Answers*” folder under “*shared folder*” (Do not recreate, if already present).
- iv. Click “*Answers*” folder and un-archive file “*OFS Basel Regulatory Capital Analytics - US_Answers*”.
- v. Create a “*BIP_REPORTS*” folder under “*shared folder*” if not already present.
- vi. Click “*BIP_REPORTS*” folder and un-archive file “*OFS Basel Regulatory Capital Analytics - US_BIP*”.
- vii. Re-Start (stop and start) the BI services.

3. Configuring FINMA

- i. Click *“shared folder”* in the left hand pane.
- ii. Select *“Un-archive option”* from File Menu and un-archive file *“OFS Basel Regulatory Capital Analytics - FINMA_Dashboard”*, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create a *“Answers”* folder under *“shared folder”* (Do not recreate, if already present)
- iv. Click *“Answers”* folder and un-archive file *“OFS Basel Regulatory Capital Analytics - FINMA_Answers”*.
- v. Create a *“BIP_REPORTS”* folder under *“shared folder”* (Do not recreate, if already present).
- vi. Click *“BIP_REPORTS”* folder and un-archive file *“OFS Basel Regulatory Capital Analytics - FINMA_BIP”*.
- vii. Re-Start (stop and start) the BI services.

4. Configuring Islamic Banking

- i. Click *“shared folder”* in the left hand pane.
- ii. Select *“Un-archive option”* from File Menu and un-archive file *“OFS Basel Regulatory Capital Analytics - IFSB_Dashboard”*, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create an *“Answers”* folder under *“shared folder”* (Do not recreate, if already present).
- iv. Click *“Answers”* folder and un-archive file *“OFS Basel Regulatory Capital Analytics - IFSB_Answers”*.
- v. Re-Start (stop and start) the BI services.

5. Configuring CBRC

- i. Click *“shared folder”* in the left hand pane.
- ii. Select *“Un-archive option”* from File Menu and un-archive file *“OFS Basel Regulatory Capital Analytics - CBRC_Dashboard”*, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create a *“BIP_REPORTS”* folder under *“shared folder”* (Do not recreate, if already present).
- iv. Click *“BIP_REPORTS”* folder and un-archive file *“OFS Basel Regulatory Capital Analytics - CBRC_BIP”*.
- v. Re-Start (stop and start) the BI services.

6. Configuring INDIA

- I. Click “*shared folder*” in the left hand pane.
- II. Select “*Un-archive option*” from File Menu and un-archive file “**OFS Basel Regulatory Capital Analytics –INDIA_Dashboard**” (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- III. Click “*shared folder*” in the left hand pane.
- IV. Select the folder called “Answers” (if not exists please create).
 - Select “Un-archive option” from File Menu and un-archive file “**OFS Basel Regulatory Capital Analytics - INDIA _Answers**” (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- V. Click “*shared folder*” in the left hand pane.
- VI. Select the folder called “BIP_REPORTS” (if not exists please create).
 - Select “Un-archive option” from File Menu and un-archive file “**OFS Basel Regulatory Capital Analytics - INDIA _BIP_Consolidated**” copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
Again Select the folder called “BIP_REPORTS” and
 - Select “Un-archive option” from File Menu and un-archive file “**OFS Basel Regulatory Capital Analytics - INDIA _BIP_Solo**” copied onto the local machine as part of introduction pre-requisite step, and click **OK**.

7. Configuring FRTB

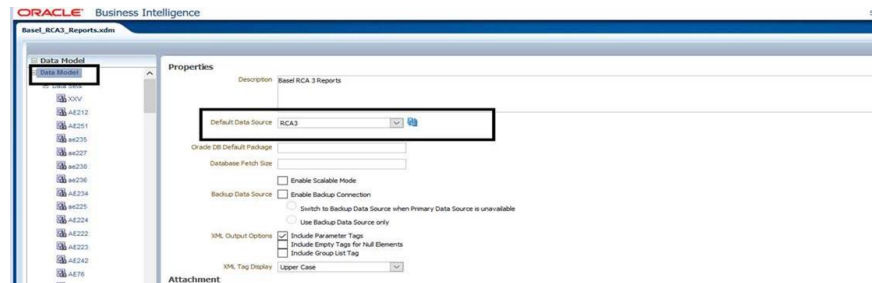
- i. Click “*shared folder*” in the left hand pane.
- ii. Select the “*Un-archive option*” from File Menu and un-archive file “**OFS Basel Fundamental Review Of Trading Book – Dashboard**”, copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- iii. Create an “Answers” folder under “*shared folder*” (Do not recreate, if already present).
- iv. Click “Answers” folder and un-archive file “**OFS Basel Fundamental Review Of Trading Book - Answers**”.
- v. Re-Start (stop and start) the BI services.

- VII. Re-Start (stop and start) the BI services.

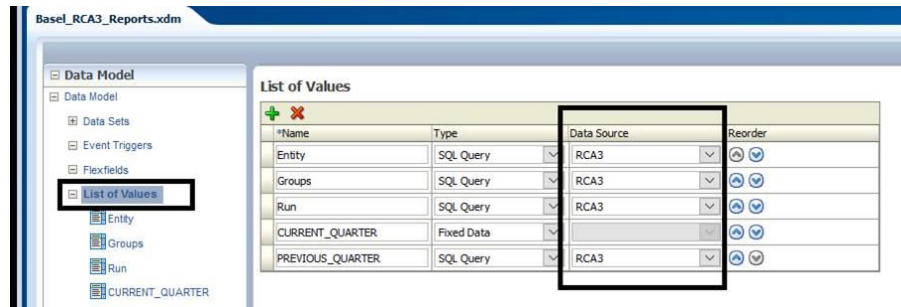
Configuring data source connection in BI Publisher for INDIA

1. Click **Administration link** (on right corner).
2. Click **Manage BI Publisher** under BI Publisher.
3. Click **JDBC Connection link** under Data Sources.
4. Add data source by name **RCA3**.

- A. Provide Driver Type (for example: Oracle 11g).
 - B. Provide Database Driver Class (for example: oracle.jdbc.OracleDriver).
 - C. Provide the Connection String (Please follow the 'demo' Connection string format, for example: jdbc:oracle:thin:@HOST:PORT:SID).
 - D. Provide Username and Password.
 - E. Click **Test Connection** to check the connection.
 - F. Click on **Apply**
5. Ensure that there is a connection string existing with the name '**RCA3**'
 6. Select the Default Data Source as **RCA3** in the **Basel_RCA3_Reports** (Path: Catalog → unarchived RCA3 folder → Edit (under India_RCAIII_DM_Solo) → click on **Data Model**) and save



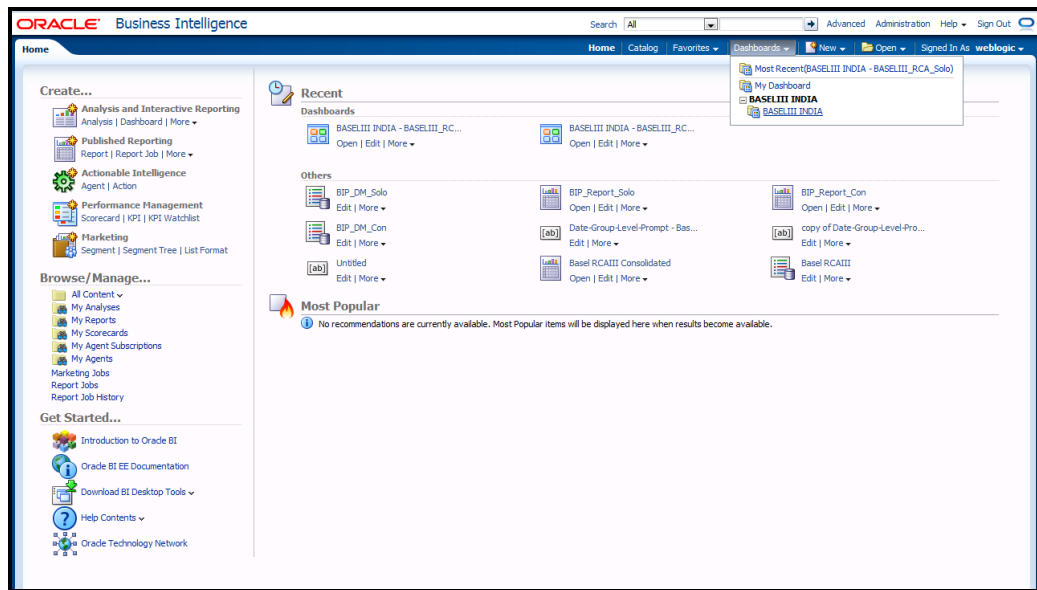
7. Select the Data Source as **RCA3** for Entity, Groups, Run and previous quarter under **List of Values** (Path: Catalog → unarchived RCA3 folder → Edit (under India_RCAIII_DM_Solo) → click on **List of Values**) and save



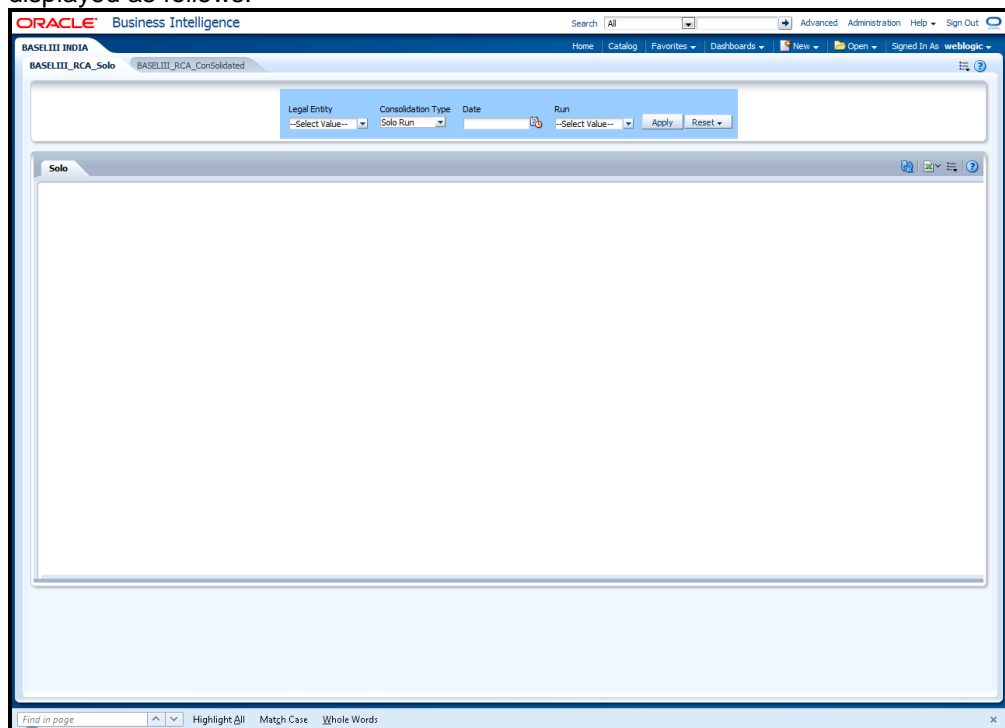
NOTE: Data must be available for FCT tables to see the BIP (for example: RCA3, FFIEC, and so on) reports in the Dashboard. Similar steps must be followed for the other Datasets (for example: ERM, FINMA)

3.2.5 Dashboard Report Verification

- a. In the *ORACLE Business Intelligence Window*: Click **Dashboards** → **BASELIII INDIA**.

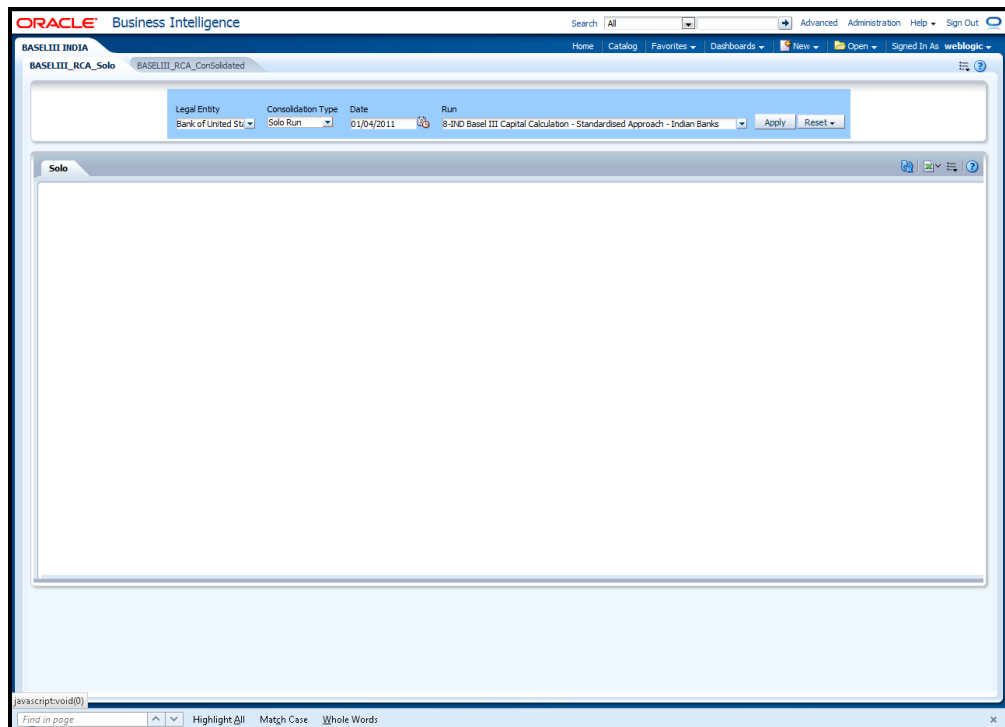


The **BASELIII_RCA_Solo** tab (and **BASELIII_RCA_Consolidated** tab) is displayed as follows.



3.2.5.1 View the RCAlII Solo Report

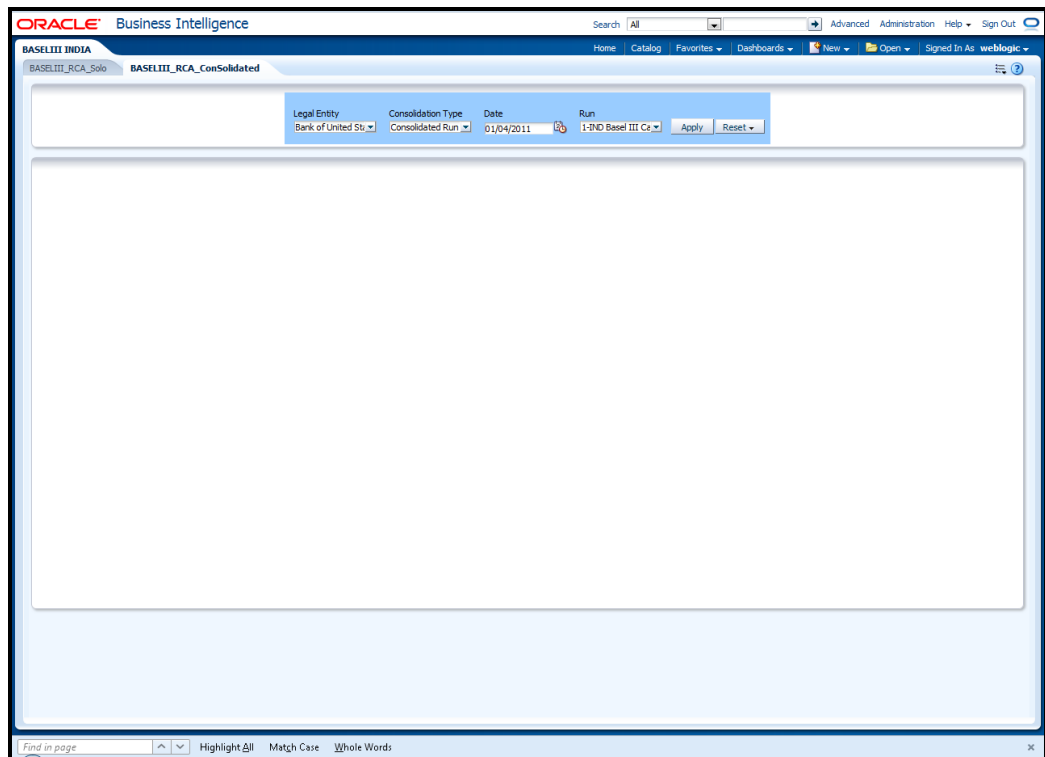
- a. Select **Legal Entity**, **Consolidation Type**, **Date**, and **Run** from the **BASELIII_RCA_Solo** tab.



- b. Click **Apply**.
The Report will get downloaded in Excel Sheet format.

3.2.5.2 View the RCAIII Consolidated Report

- a. Select **Legal Entity**, **Consolidation Type**, **Date**, and **Run** from the **BASELIII_RCA_Consolidated** tab.



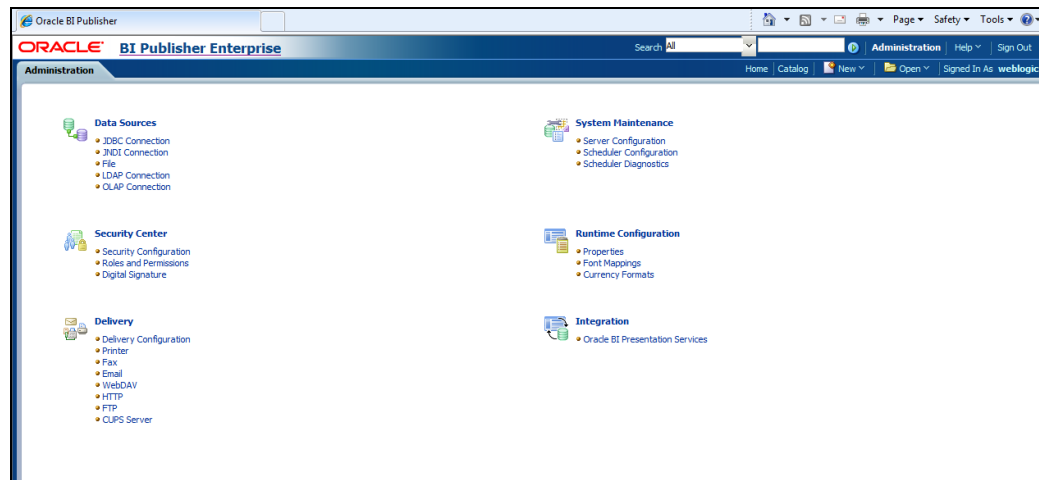
- b. Click **Apply**.
The Report will get downloaded in Excel Sheet format.

3.2.6 Installation of Images (Only for New Installation):

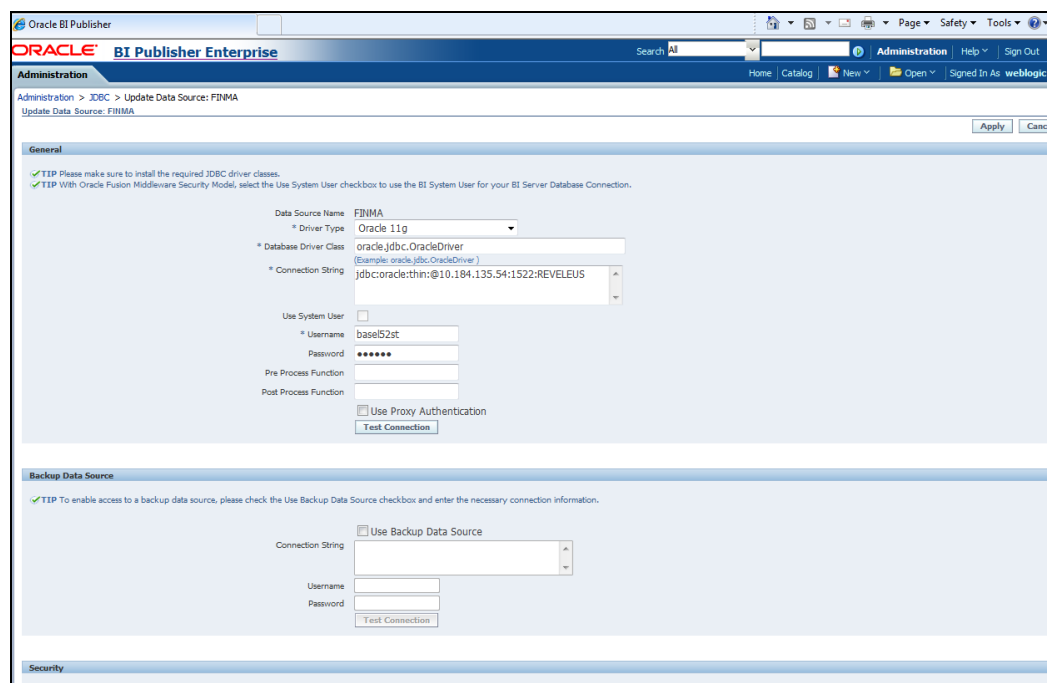
- a. Uncompress the file “OFS Basel Regulatory Capital Analytics <version number> - Images.zip” (this zip folder is available on the local machine as part of introduction pre-requisite step) and copy all the images to the folder <OBIEE Installation Path>\Oracle_BI1\bifoundation\web\app\res\s_blafp\images.
- b. Uncompress the file “OFS Basel Regulatory Capital Analytics <version number> - Images.zip” and copy all the images to the folder <OBIEE Installation path>\user_projects\domains\bifoundation_domain\servers\bi_server1\tmp\WL_user\analytics_11.1.1\7dezi\war\res\s_blafp\images.
- c. Re-Start (stop and start) the BI services.

3.2.7 BI Publisher Reports (Only for New Installation):

- a. Type the link for Oracle BI Publisher link.
For example: http://URL:<port_number>/xmlpserver
- b. Login through Administrator user ID and password.
- c. Click **Administration** (available at top right of the page).
- d. Click **JDBC Connection**, available under Data Sources.



e. Click **Add Data Source**.



Give Data Source name as “**FINMA**”.

Driver Type – According to available database type to connect.

Connection String – Put the *HOST*, *PORT* and *SID* of database in the given format.

For example: (Oracle 11g Driver)
 :(*jdbc:oracle:thin:@10.184.200.32:1521:OFSAA*)

Username/Password – Put the database user id and password.

Click **Test Connection**. “*Connection established successfully*” appears.

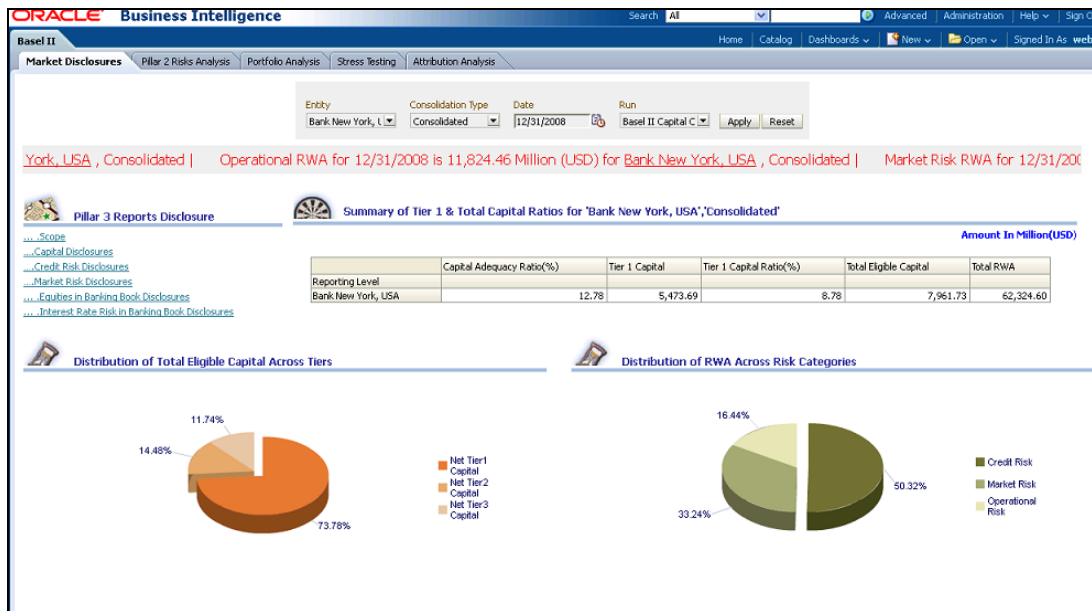
Click **Apply**.

Ignore other settings. **Guest** settings can be applied, according to usage.

- f. Similarly add two more data sources with names “**ERM**” and “**CBRC**”, as described in the above step e.
- g. Repeat the same steps [5 to 7](#) of Section 3.2.4 in the Oracle BI Publisher.

3.3 Post configuration verification steps

- a. Log into Analytics and check if the screen looks similar to the diagram shown below.

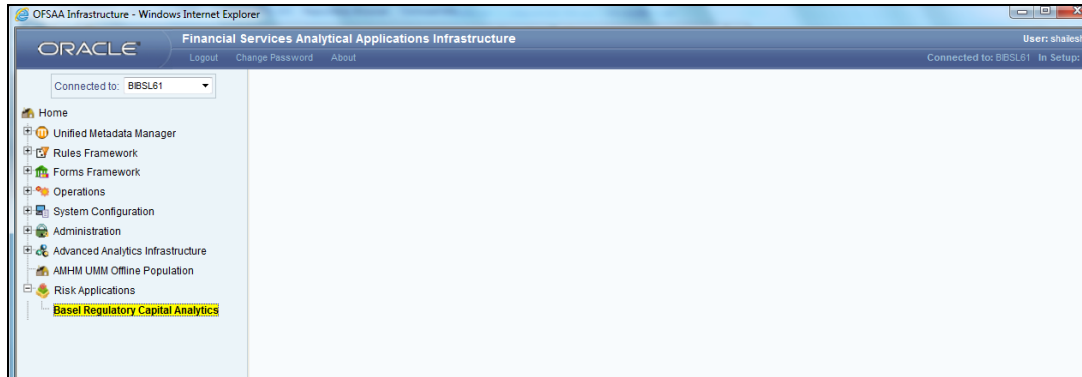


- b. Click each of the dashboard links, and check if all the links are visible.

3.4 Configuring OBIEE link in OFSAAI Framework

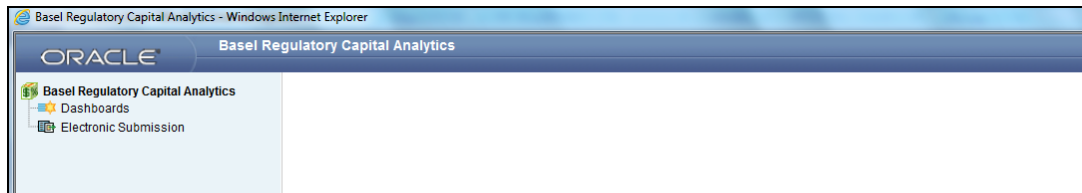
The Dashboard (OBIEE) link is accessed from OFSAAI Framework. Log in to the OFSAAI application. Click the “+” sign next to **Risk Applications** from LHS (left hand side) menu.

Under **Risk Applications**, click **Basel Regulatory Capital Analytics** option.



The Basel Regulatory Capital analytics page appears. On the LHS, you will have two options

- Dashboards
- Electronic Submission



To Configure the Dashboard (OBIEE) link, select the “CONFIGURATION” table. In this table, provide the OBIEE URL into the column ‘Paramname’ (that is, against paramname = OBIEE_URL). The paramvalue needs to be replaced with the required URL. The format of the URL to be replaced depends on the IE configuration as `http://<ipaddress>:<port>/analytics` or `https://<ipaddress>:<port>/analytics`.

Replacing the URL completes the configuration process for the dashboard link.

If you encounter any problems during setup, contact OFSAA Support at [Oracle Support](#)

3.5 Oracle Financial Services Electronic Submission Administration Activities

Oracle Financial Services Electronic Submission Utility (FFIEC Submission) generates text file in the format specified by the FFIEC regulators. This utility is integrated with Oracle Financial Services (OFS) Basel Regulatory Capital Solution. This utility will prepare the text file compatible with Electronic Format, for all FFIEC Schedules and all the Edit Checks.

The Schedules undergo workflow process which involves Editing and Submitting the Schedules of a selected Report for Authorization for the changes made. The editing and submitting of Schedules can only be done by roles which have Analyst Permission for the selected Schedules. Authorization and rejection can be done by roles having Authorization Permission for the selected Schedules. Super Users can only generate & submit E-file and can perform delete operation for a given report. They can reset an authorized schedule to its draft condition.

User Administrator creates user definitions, user groups, maintain profiles, authorize users and UserGroups, and map users to groups, domains and roles.

System Administrator is responsible for configuring the Mail Utility and Seeded data for User Roles.

Note: It is recommended to click **Close** button given on the Forms page and not close the browser tab.

3.6 User Administrator

To create users, user groups, map users to user groups, and so on, refer to the following topics.

- User Maintenance
- UserGroup Maintenance
- User UserGroup Map
- User Authorization
- User Group Authorization
- UserGroup Role Map

3.6.1 User Maintenance


User Maintenance facilitates you to create user definitions, View, Manage, Modify, and Delete user information. You can access User Maintenance by expanding **User Administrator** section within the tree structure of the LHS menu.

The *User Maintenance* screen displays user details such as User ID, Name, Profile Name, Start and End dates. You can also identify the user status if enabled, to access the Infrastructure system.

You can also make use of the Search and Pagination options to search for a specific user or view list of existing users within the system.

3.6.1.1 Add User

To add a user definition in the *User Maintenance* screen:

1. Select  button from the User Maintenance tool bar. **Add** button is disabled if you select any User ID in the grid. The *New User* screen is displayed.

User Maintenance
User Maintenance > User Definition (add mode)

User Maintenance

User ID *	JohnAdmin	User Name *	John K
Address	Nottingham Road, New York	Date of Birth	07/07/1970
Designation	Administrator	Profile Name *	Profile for the Administrator
Start Date *	07/29/2011	End Date *	07/29/2015
Password *	*****		

Notification Time

Start	09:00	End	08:00
Email ID	john_k@email.com	Mobile No	+858436947
Pager No	6585201266		

Enable User

Enable User	<input checked="" type="checkbox"/>	Login on Holidays	<input checked="" type="checkbox"/>
-------------	-------------------------------------	-------------------	-------------------------------------

Save Cancel

User Info

Created By		Created Date	
Last Modified By		Last Modified Date	

2. Enter the user details as tabulated.

Field	Description
Fields marked in red asterisk (*) are mandatory.	
User ID	Enter a unique user id. Ensure that there are no special characters and extra spaces in the id entered.
User Name	Enter the user name. The user name specified here will be displayed on the Infrastructure splash screen. Ensure that the User Name does not contain any special characters or spaces except "_", "'", and ".".
Contact Address	Enter the contact address of the user. It can be the physical location from where the user is accessing the system. Ensure that Contact Address does not contain any special characters except ".", "#", "-", ";", ":".
Date Of Birth	Specify the date of birth. You can use the popup 'calendar' to enter the date.
Designation	Enter the user designation. Ensure that Designation does not contain any special characters except "_", ".", and "-".
Profile Name	Select the profile name by clicking on the drop down list.
User Start Date	Specify the user start date based on the day slot the user is enabled to access the system. Ensure that User Start Date is greater than today's date. You can use the popup 'calendar' to enter the date.
User End Date	Specify the user end date based on month and year when the user Id expires. Ensure that user End Date is greater than User Start Date. You can use the popup 'calendar' to enter the date.
Password	Enter the default password for the user for the initial login. User needs to change the default password during the first login. A user is denied access in case the user has forgotten the password or enters the wrong password for the specified number of attempts (as defined in the <i>Configuration</i> screen). To enable access, enter a new password here.
Notification Time	(Optional) Specify the notification start and end time within which the user can be notified with alerts.
E-mail ID	Enter the e-mail address of the user. This is mandatory field for FFIEC mail utility.
Mobile No	(Optional) Enter the mobile number of the user.
Pager No	(Optional) Enter the pager number of the user.
Enable User	Select the checkbox to allow user to access the system. A deselected checkbox denies access to the user.


Field	Description
Login on Holidays	Select the checkbox to allow users to access the system on holidays. A deselected checkbox denies access to the user on holidays.

3. Click **Save** to upload the user details.

The new User details are populated in the *User Authorization* screen which has to be authorized by System Authorizers. Once authorized, the **User** details are displayed in *User Maintenance* screen and can then be mapped to the required user group in the [User UserGroup Map](#) screen.

3.6.1.2 View User Details


You can view individual user details at any given point. To view the existing function details in the *User Maintenance* screen:

1. Select the checkbox adjacent to the User ID.
2. Click  button in the User Maintenance tool bar.

The *View User Details* screen is displayed with details such as User ID, User Name, Address, Date of Birth, Designation, Profile Description, Start and End Date in which the user can access Infrastructure system. The *View User Details* screen also displays notifications details and status if enable to access the system on holidays.

3.6.1.3 Modify User Details

To update the existing user details in the *User Maintenance* screen:

1. Select the checkbox adjacent to the User ID whose details are to be updated.
2. Click  button in the User Maintenance tool bar.

The *Edit User Details* screen is displayed.


3. Update the required information. *For more details, refer [Add User](#).*

NOTE: You cannot edit the User ID. You can view the modifications once the changes are authorized. Also, a new password must be provided during the user details modification.

4. Click **Save** to save the changes.

3.6.1.4 Delete User Details


You can remove the user definition(s) which are created by you and which are no longer required in the system, by deleting from the *User Maintenance* screen.

1. Select the checkbox adjacent to the user ID whose details are to be removed.
2. Click  button in the User Maintenance tool bar.
3. Click **OK** in the information dialog to confirm deletion.

NOTE: User can access the application until the delete request is authorized.

3.6.1.5 Add User Attributes

To add attributes to a user in the *User Maintenance* screen:

1. Select the checkbox adjacent to the User ID for whom you wish to add additional attributes.
2. Click  button in the User Maintenance tool bar. The *User Maintenance Attributes* screen is displayed.
3. In the *User Maintenance Attributes* screen, enter additional attributes in the field adjacent to the user name.

The attribute fields that are displayed in this window can be configured depending on your requirements. For more information, see *Function Mapping Codes* in the OFSAAI User Guide.

4. Click **Save** to upload the changes.

3.6.2 UserGroup Maintenance

UserGroup Maintenance facilitates you to create view, edit, delete, and map user(s) to specific groups. You can maintain and modify the user group information within the *UserGroup Maintenance* screen.


You can access UserGroup Maintenance by expanding **User Administrator** section within the tree structure of LHS menu.

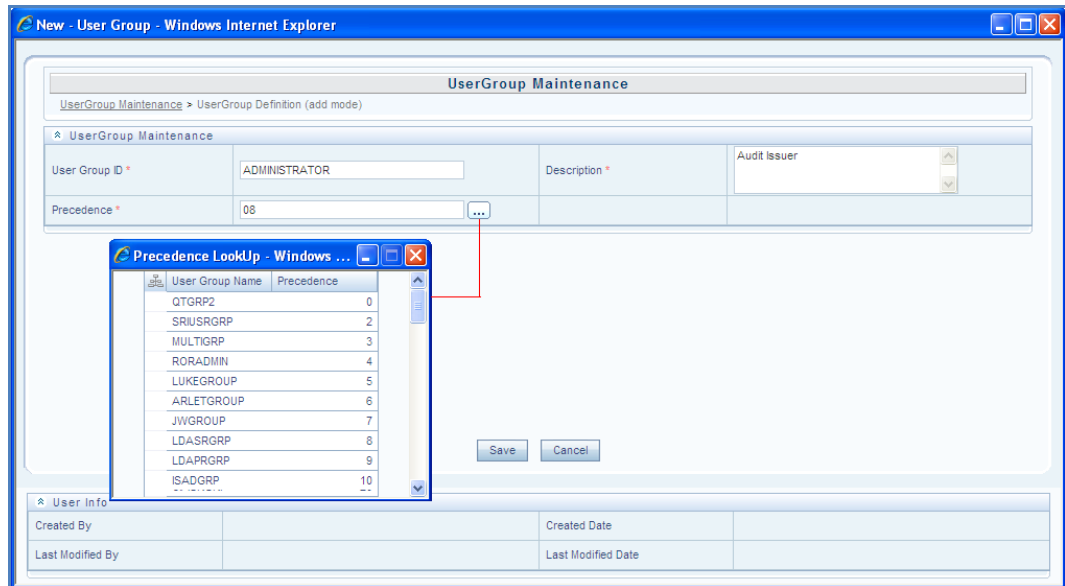
UserGroup Maintenance screen displays details such as User Group ID, Description, Precedence, and the number of Mapped Users.

You can also make use of Search and Pagination options to search for a specific user group or view the list of existing user groups within the system.


3.6.2.1 Add User Group

To add a User Group in the *UserGroup Maintenance* screen:

1. Select  from the User Group tool bar. The **Add** button is disabled if you have selected any UserGroup ID in the grid. The *New User Group* screen is displayed.



2. Enter the details as tabulated.


Field	Description
User Group ID	Specify a unique id for the user group. Ensure that there are no special characters and extra spaces in the id entered.
Description	Enter a description for the user group.
Precedence	Enter the Precedence value. You can click  button to Lookup for the existing precedence values applied to the various user groups.

NOTE: The lower the value in the precedence column, the higher is precedence. A user may be mapped to multiple user groups and hence the precedence value is required if Group Based Hierarchy Security setting is selected in the *Configuration* screen.

3. Click **Save** to upload the user group details. The new User Group details need to be authorized before associating users to the user group created.

3.6.2.2 View UserGroup Details


You can view individual usergroup details at any given point. To view the existing usergroup details in the *UserGroup Maintenance* screen:

1. Select the checkbox adjacent to the User Group ID.
2. Click  button in the User Group tool bar.

The *View UserGroup Details* screen is displayed with the details such as User Group ID, Description, and Precedence value.


3.6.2.3 Modify User Group

To update the existing usergroup details in the *UserGroup Maintenance* screen:

1. Select the usergroup whose details are to be updated by clicking on the checkbox adjacent to the User Group ID.
2. Click  button in the User Group tool bar. Edit button is disabled if you have selected multiple groups.
3. Edit the required User Group details except for UserGroup ID which is not editable. For more information refer [Add User Group](#).
4. Click **Save** to upload changes.

3.6.2.4 Delete User Group

You can remove user group definition(s) which are created by you, which do not have any mapped users, and which are no longer required, by deleting from the *Usergroup Maintenance* screen.

1. Select the checkbox adjacent to the user group ID(s) whose details are to be removed.
2. Click  button in the User Group tool bar.
3. Click **OK** in the information dialog to confirm deletion.

NOTE: UserGroups cannot be deleted if any requests (Domain map/unmap and Role map/unmap) are pending for authorization or any users are mapped to it.

3.6.3 User UserGroup Map

User UserGroup Map facilitates you to map user(s) to specific user group which in turn is mapped to a specific Information Domain and role. Every UserGroup mapped to the infodom needs to be authorized. Else, it cannot be mapped to users.

User UserGroup Map screen displays details such as User ID, Name, and the corresponding Mapped Groups. You can view and modify the existing mappings within the *User UserGroup Maintenance* screen.

You can access User UserGroup Map by expanding User Administrator section within the tree structure of LHS menu.

You can also make use of Search and Pagination options to search for specific users or view the list of existing usergroup map within the system.

3.6.3.1 View Mapped Users






You can view usergroup mapping of a particular user at any given point.

To view the existing usergroup map details in the *User UserGroup Map* screen select the checkbox adjacent to the User ID. The list of group(s) to which the selected user has been mapped is displayed under *Mapped Groups* grid.

3.6.3.2 Map/Unmap Users

User UserGroup Map facilitates you to map user(s) to specific user group which in turn is mapped to a specific Information Domain and Role. Every UserGroup mapped to the Information Domain needs to be authorized. Otherwise it cannot be mapped to users.

To map/unmap users in *User UserGroup Map* screen:

1. Select the checkbox adjacent to the User ID.
2. Click  button in the *Mapped Groups* grid. The *User UserGroup Mapping* screen is displayed.
3. In the *User UserGroup Mapping* screen, you can search for a UserGroup using the Search field and edit the mapping.
 - To map a user to a group, select the UserGroup and click . You can press **Ctrl** key for multiple selections.
 - To map all the UserGroups to a user, click .
 - To remove a UserGroup mapping for a user, select the UserGroup from Select Members pane and click .
 - To remove all the group mappings of a user, click .
4. Click **OK** to save the mappings and return to *User UserGroup Map* screen.

NOTE: UserGroup is displayed in the *User UserGroup Mapping* screen only if it is mapped to at least one Domain and Role.

3.6.4 Profile Maintenance


Profile Maintenance facilitates you to create profiles, specify the time zones, specify the working days of the week and map holiday's schedule. *Profile Maintenance* screen displays the existing profiles with details such as the Profile Code, Profile Name, Time Zone, Workdays of Week, Holiday Time Zone, and mapped Holidays. In the *Profile Maintenance* screen you can add, view, edit, and delete user profile definitions.

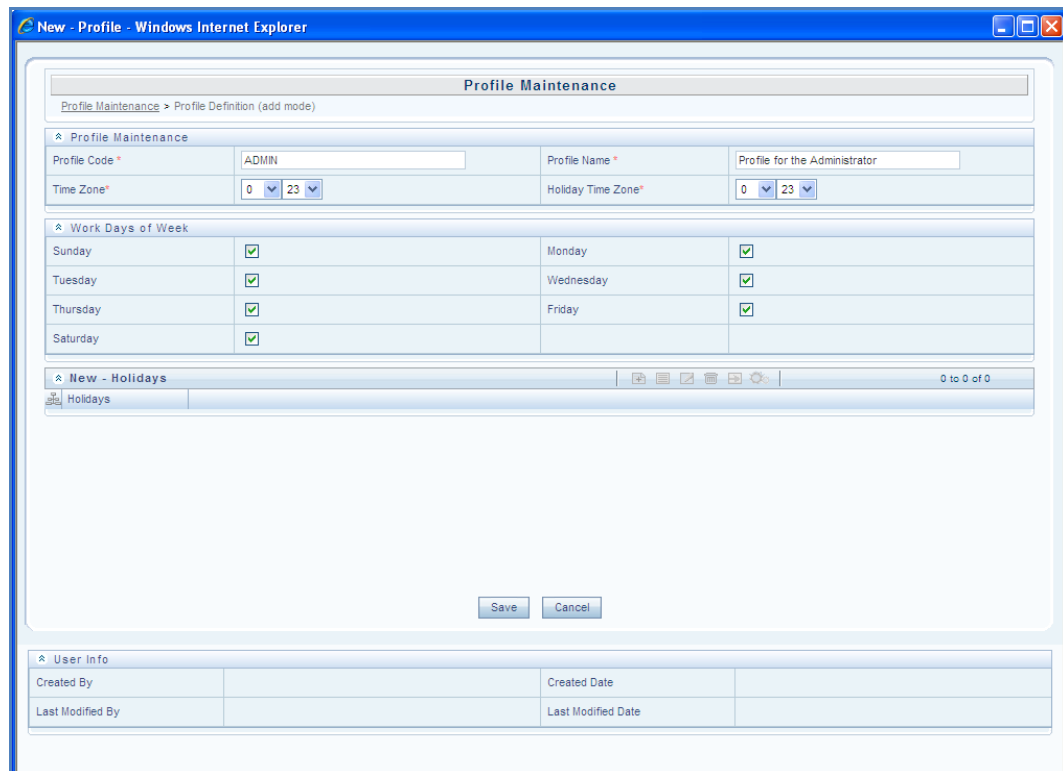
You can access Profile Maintenance by expanding **User Administrator** section within the tree structure of LHS menu.

You can also make use of Search and Pagination options to search for specific profile or view the list of existing profiles within the system.

3.6.4.1 Add Profile

To add a profile in the *Profile Maintenance* screen:

1. Select  from the Profile Maintenance tool bar. **Add** button is disabled if you have selected any Profile Code check box in the grid.



The screenshot shows the 'New Profile' screen in Internet Explorer. The browser title is 'New - Profile - Windows Internet Explorer'. The page title is 'Profile Maintenance'. The breadcrumb is 'Profile Maintenance > Profile Definition (add mode)'. The form contains several sections:

- Profile Maintenance:** Profile Code * (ADMIN), Profile Name * (Profile for the Administrator), Time Zone* (0-23), Holiday Time Zone* (0-23).
- Work Days of Week:** A table with checkboxes for Sunday, Tuesday, Thursday, Saturday, Monday, Wednesday, and Friday, all of which are checked.
- New - Holidays:** A table for adding holidays.
- User Info:** Fields for Created By, Last Modified By, Created Date, and Last Modified Date.

At the bottom are 'Save' and 'Cancel' buttons.






2. The *New Profile* screen is displayed. Enter the details as tabulated.

Field	Description
Profile Code	Enter a unique profile code based on the functions that the user executes. For example, specify AUTH if you are creating an authorizer profile.
Profile Name	Enter a unique profile name. Ensure that Profile Name does not contain any special characters except ".", "(", ")", "_", "-".
Time Zone	Select the Start and End time zone from the drop-down list. Time zones are hourly based and indicate the time at which the user can access the system.
Holiday Time Zone	Select the Holiday Start and End time zone from the drop-down list. Time zones are hourly based and indicate the time at which the user can access the system on holidays.
Work Days of Week	Select the work days of a week by clicking on the check box adjacent to week days. The specified time zones will be applicable to the selected days.

3. Click **Save** to save the profile.


3.6.4.2 Map Holidays

To enable user to access the Infrastructure system during holidays, map the profile to the holiday's schedule. For the user to access the system on holidays, the **Login on Holidays** checkbox in the *User Maintenance* screen must be checked.

1. Click  button in the *New Holidays* grid. *Holiday Mapping* screen is displayed.
The *Holiday Mapping* screen displays the holidays that are added through the **Holiday Maintenance** section.
2. To map a holiday, you can do the following:
 - To map holiday to the user profile, select from the list and click .
 - To map all the listed holidays to the user profile, click .
 - To remove holiday mapping to user profile, select from the list and click .
 - To remove entire holiday mapping for the user profile, click .
3. Click **OK** to save the mapping.

3.6.4.3 View Profile

You can view the profile of a particular user at any given point. To view the existing user profile details in the *Profile Maintenance* screen:


1. Select the checkbox adjacent to the Profile Code.
2. Click  button in the Profile Maintenance tool bar.

The *Profile Maintenance* screen displays profile of the user with the holiday mapping details.

3.6.4.4 Modify Profile


You can modify all the details except **Profile Code** and **Profile Name** of individual profiles at any given point of time.

To edit a user profile in the *Profile Maintenance* screen:

1. Select the checkbox adjacent to the Profile Code.
2. Click  button in the Profile Maintenance tool bar.
3. Edit the user profile as required. For more information refer [Add Profile](#).
4. Click **Save** to upload changes.

3.6.4.5 Delete Profile

You can remove user profile definition(s) which are created by you and which are no longer required in the system, by deleting from the *Profile Maintenance* screen.

1. Select the checkbox adjacent to the Profile Code(s) whose details are to be removed.
2. Click  button in the Profile Maintenance tool bar.
3. Click **OK** in the information dialog to confirm deletion.

3.6.5 User Authorization

User Authorization function facilitates system authorizers to authorize and allow user(s) created or modified by system administrator to access the Infrastructure system. Whenever a new user is created or an authorized user details are updated, the user has to be authorized by the system authorizers to allow access to the Infrastructure system. The function also restricts access to unauthorized user(s).

- As a system Authorizer, you can:
 - View the available user ID's which are to be authorized.
 - Authorize or reject users to access the system.

- Authorize or reject modification request of Users.
- View the current updated and previous user details for authorization.
- Authorize based on the user ID's created by Systems Administrator.
- As a user, you can login to the Infrastructure system only if authorized by the system Authorizer.



You can access *User Authorization* screen by expanding User Administrator section within the tree structure of LHS menu.

The *User Authorization* screen displays a list of available users for Authorization. By default, the users will be displayed in alphabetical order of the User ID's with the other details such as User ID, Name, User Start Date, and User Expiry Date.

You can also make use of Search and Pagination options to search for specific users.

3.6.5.1 Authorize or Reject User(s)

In the *User Authorization* screen, do the following:

1. Select User ID which has to be authorized. The screen is refreshed and the details are displayed below.
2. In the User Authorization tool bar,
 - Click  (authorize) button to authorize a user(s).
 - Click  (reject) button to reject a user(s).
3. Click **OK** in the information dialog to confirm authorization or rejection. On processing, a system message is displayed.

3.6.6 User Group Authorization

User Group Authorization function facilitates system authorizers to authorize or reject the user groups listed in the *User Group Authorization* screen.

- As a system Authorizer, you can:
 - View the list of mapped/unmapped user(s) to be authorized.
 - Authorize or reject mapping/unmapping of user group(s) to a role or a domain.



You can access *User Group Authorization* screen by expanding **User Administrator** section within the tree structure of LHS menu.

The *User Group Authorization* screen displays a list of available user groups for Authorization. By default, the user groups are displayed in alphabetical order of the Mapped User Groups with the other details such as Mapped/Unmapped Users, Mapped/Unmapped Roles, and Mapped/Unmapped DSNs.

You can also make use of Search and Pagination options to search for specific user group.

3.6.6.1 Authorize or Reject User Group(s)

In the *User Group Authorization* screen, do the following:

1. Select the required **User Group ID** for authorization.
The Mapped/Unmapped Users, Mapped/Unmapped Roles, and Mapped/Unmapped DSNs corresponding to the selected User Group are displayed in the respective grids.
2. Select the checkbox adjacent to the mapped or unmapped group details.
3. In the User Authorization tool bar,
 - Click  (authorize) button to authorize a user group(s).
 - Click  (reject) button to reject a user group(s).
4. Click **OK** in the information dialog to confirm authorization or rejection. On processing, a system message is displayed.

3.6.7 UserGroup Domain Map


UserGroup Domain Map facilitates System Administrators to view the available user groups and map the required Domain to User Group(s). System Administrators can also remove user group mapping for specific domain or map additional domains to a specific user group to ensure confidentiality of restricted Information Domains.





You can access *UserGroup Domain Map* screen by expanding **User Administrator** section within the tree structure of LHS menu.

The *UserGroup Domain Map* screen displays a list of available user groups in alphabetical order with the User Group ID and Description. On selecting a user group, the list of available mapped domains are displayed.

You can also make use of Search and Pagination options to search for specific usergroup or view the list of existing usergroups within the system.

To map a UserGroup to a Domain, do the following:

1. Select the checkbox adjacent to the required UserGroup ID. The *UserGroup Domain Map* screen is refreshed to display the existing mapped domains.
2. Click  button in the Mapped Domains section tool bar. The *UserGroup Domain Map* screen is displayed.
3. In the *UserGroup Domain Map* screen, you can search for a Domain using the Search field and edit the mapping.

- To map Domains to a User Group, select the Domain from the Members list and click . You can press **Ctrl** key for multiple selections.
 - To map all the Domains to a User Group, click .
 - To remove mapping for a user group, select the Domain from Select Members list and click .
 - To remove all Domains mapped to UserGroup, click .
4. Click **OK** to save the mappings and return to *UserGroup Domain Map* screen.

3.6.8 UserGroup Role Map

The roles are provided as seeded data. These roles are defined as per each schedule.

ROLE CODE	ROLE NAME	ROLE DESCRIPTION
AANALYST	Schedule A Analyst Role	Role for Analyst Schedule A
AAUTHORIZE	Schedule A Auth Role	Role for Auth Schedule A
ASUPERUSR	Schedule A SuperUsr Role	Role for SuperUsr Schedule A
AVIEWER	Schedule A View Role	Role for View Schedule A
BANALYST	Schedule B Analyst Role	Role for Analyst Schedule B
BAUTHORIZE	Schedule B Auth Role	Role for Auth Schedule B
BSUPERUSR	Schedule B SuperUsr Role	Role for SuperUsr Schedule B
BVIEWER	Schedule B View Role	Role for View Schedule A
CANALYST	Schedule C Analyst Role	Role for Analyst Schedule C
CAUTHORIZE	Schedule C Auth Role	Role for Auth Schedule C
CSUPERUSR	Schedule C SuperUsr Role	Role for SuperUsr Schedule C
CVIEWER	Schedule C View Role	Role for View Schedule C
DANALYST	Schedule D Analyst Role	Role for Analyst Schedule D
DAUTHORIZE	Schedule D Auth Role	Role for Auth Schedule D
DSUPERUSR	Schedule D SuperUsr Role	Role for SuperUsr Schedule D
DVIEWER	Schedule D View Role	Role for View Schedule D
EANALYST	Schedule E Analyst Role	Role for Analyst Schedule E

ROLE CODE	ROLE NAME	ROLE DESCRIPTION
EAUTHORIZE	Schedule E Auth Role	Role for Auth Schedule E
ECANALYST	Schedule EC Analyst Role	Role for Analyst Edit Checks
ECAUTHORIZ	Schedule EC Auth Role	Role for Auth Edit Checks
ECSUPERUSR	Schedule EC SuperUsr Role	Role for SuperUs Edit Checks
ECVIEWER	Schedule EC View Role	Role for View Edit Checks
EFILEACCES	Generate and View E-File	Role to Generate and View E-File
ESUPERUSR	Schedule E SuperUsr Role	Role for SuperUsr Schedule E
EVIEWER	Schedule E View Role	Role for View Schedule E
FANALYST	Schedule F Analyst Role	Role for Analyst Schedule F
FAUTHORIZE	Schedule F Auth Role	Role for Auth Schedule F
FSUPERUSR	Schedule F SuperUsr Role	Role for SuperUsr Schedule F
FVIEWER	Schedule F View Role	Role for View Schedule F
GANALYST	Schedule G Analyst Role	Role for Analyst Schedule G
GAUTHORIZE	Schedule G Auth Role	Role for Auth Schedule G
GSUPERUSR	Schedule G SuperUsr Role	Role for SuperUsr Schedule G
GVIEWER	Schedule G View Role	Role for View Schedule G
HANALYST	Schedule H Analyst Role	Role for Analyst Schedule H
HAUTHORIZE	Schedule H Auth Role	Role for Auth Schedule H
HSUPERUSR	Schedule H SuperUsr Role	Role for SuperUsr Schedule H
HVIEWER	Schedule H View Role	Role for View Schedule H
IANALYST	Schedule I Analyst Role	Role for Analyst Schedule I
IAUTHORIZE	Schedule I Auth Role	Role for Auth Schedule I
ISUPERUSR	Schedule I SuperUsr Role	Role for SuperUsr Schedule I
IVIEWER	Schedule I View Role	Role for View Schedule I
JANALYST	Schedule J Analyst Role	Role for Analyst Schedule J
JAUTHORIZE	Schedule J Auth Role	Role for Auth Schedule J

ROLE CODE	ROLE NAME	ROLE DESCRIPTION
JSUPERUSR	Schedule J SuperUsr Role	Role for SuperUsr Schedule J
JVIEWER	Schedule J View Role	Role for View Schedule J
KANALYST	Schedule K Analyst Role	Role for Analyst Schedule K
KAUTHORIZE	Schedule K Auth Role	Role for Auth Schedule K
KSUPERUSR	Schedule K SuperUsr Role	Role for SuperUsr Schedule K
KVIEWER	Schedule K View Role	Role for View Schedule K
LANALYST	Schedule L Analyst Role	Role for Analyst Schedule L
LAUTHORIZE	Schedule L Auth Role	Role for Auth Schedule L
LSUPERUSR	Schedule L SuperUsr Role	Role for SuperUsr Schedule L
LVIEWER	Schedule L View Role	Role for View Schedule L
MANALYST	Schedule M Analyst Role	Role for Analyst Schedule M
MAUTHORIZE	Schedule M Auth Role	Role for Auth Schedule M
MSUPERUSR	Schedule M SuperUsr Role	Role for SuperUsr Schedule M
MVIEWER	Schedule M View Role	Role for View Schedule M
NANALYST	Schedule N Analyst Role	Role for Analyst Schedule N
NAUTHORIZE	Schedule N Auth Role	Role for Auth Schedule N
NSUPERUSR	Schedule N SuperUsr Role	Role for SuperUsr Schedule N
NVIEWER	Schedule N View Role	Role for View Schedule N
OANALYST	Schedule O Analyst Role	Role for Analyst Schedule O
OAUTHORIZE	Schedule O Auth Role	Role for Auth Schedule O
OSUPERUSR	Schedule O SuperUsr Role	Role for SuperUsr Schedule O
OVIEWER	Schedule O View Role	Role for View Schedule O
PANALYST	Schedule P Analyst Role	Role for Analyst Schedule P
PAUTHORIZE	Schedule P Auth Role	Role for Auth Schedule P
PSUPERUSR	Schedule P SuperUsr Role	Role for SuperUsr Schedule P
PVIEWER	Schedule P View Role	Role for View Schedule P

ROLE CODE	ROLE NAME	ROLE DESCRIPTION
QANALYST	Schedule Q Analyst Role	Role for Analyst Schedule Q
QAUTHORIZE	Schedule Q Auth Role	Role for Auth Schedule Q
QSUPERUSR	Schedule Q SuperUsr Role	Role for SuperUsr Schedule Q
QVIEWER	Schedule Q View Role	Role for View Schedule Q
RANALYST	Schedule R Analyst Role	Role for Analyst Schedule R
RAUTHORIZE	Schedule R Auth Role	Role for Auth Schedule R
RSUPERUSR	Schedule R SuperUsr Role	Role for SuperUsr Schedule R
RVIEWER	Schedule R View Role	Role for View Schedule R
SANALYST	Schedule S Analyst Role	Role for Analyst Schedule S
SAUTHORIZE	Schedule S Auth Role	Role for Auth Schedule S
SSUPERUSR	Schedule S SuperUsr Role	Role for SuperUsr Schedule S
SVIEWER	Schedule S View Role	Role for View Schedule S
UPLOADEDIT	Upload Report	Role to Upload Report
UPLOADVIEW	View Report	Role to view Upload Report
CALL31RCV	View Call 31 RC Role	Role for view Call 31 RC
CL31RCGV	View Call 31 RCG	Role for view Call 31 RCG
CL31RCRP2	View Call 31 RCR Part 2	Role for view Call 31 RCR Part 2
CL31RCR1BV	View Call 31 RCR Part 1B	Role for view Call 31 RCR Part 1B
CALL31RCRV	View Call 31 RCR Role	Role for view Call 31 RCR
CL31RIBP2V	View Call 31_R_I_B P2	Role for view Call 31_R_I_B P2
CALL41RCV	View Call 41 RC Role	Role for view Call 41 RC
CALL41RCRV	View Call 41 RCR Role	Role for view Call 41 RCR
C41RCRP1BV	View Call 41 RCR Part 1B	Role for view Call 41 RCR Part 1B
CL41RCRP2V	View Call 41 RCR Part 2	Role for view Call 41 RCR Part 2
CL41RIBP2V	View Call 41_R_I_B P2	Role for view Call 41_R_I_B P2

ROLE CODE	ROLE NAME	ROLE DESCRIPTION
CL41RCGV	View Call 41 RCG	Role for view Call 41 RCG
FRY9CHCV	View FRY 9C HC Role	Role for view FRY 9C HC
FRY9CHCRV	View FRY 9C HCR Role	Role for view FRY 9C HCR
FRYRCP1BV	View FRY 9C_RC PART IB	Role for view FRY 9C_RC PART IB
FRY9CHCRP2	View FRY 9C HCR Part 2	Role for view FRY 9C HCR Part 2
FY9CHIBP2V	View FRY 9C_HI_B_Part 2	Role for view FRY 9C_HI_B_Part 2
FRY9CHCGV	View FRY 9C_HC_G	Role for view FRY 9C_HC_G
CALL31RCV	View Call 31 RC Role	Role for view Call 31 RC
CL31RCGV	View Call 31 RCG	Role for view Call 31 RCG

NOTE: A user group that can edit a specific schedule cannot have authorize or super user permissions. Similarly, a user group with authorize permission cannot have super user or edit permission.

UserGroup Role Map facilitates System Administrators to map Role(s) to specific User Group(s). Each role has a defined function and any user(s) mapped to the role has to perform only those functions.

For example, the table below lists the user group mapped to a specific role.






GROUP CODE	ROLE CODE
ADMIN	SYSADM
AUTH	SYSATH
CWSADM	CWSADMIN

You can access *UserGroup Role Map* screen by expanding **User Administrator** section within the tree structure of LHS menu.

The *UserGroup Role Map* screen displays a list of available user groups in alphabetical order with the User Group ID and Description. On selecting a user group, the list of available mapped roles are displayed.

You can also make use of Search and Pagination options to search for specific usergroup or view the list of existing usergroups within the system.

To map a Role to User Group, follow the below steps:

1. Select the checkbox adjacent to the required UserGroup ID. The *UserGroup Role Map* screen is refreshed to display the existing mapped roles.
2. Click  button in the Mapped Roles section tool bar. The *UserGroup Role Map* screen is displayed.
3. In the *UserGroup Role Map* screen, you can search for a Role using the Search field and edit the mapping.
 - To map Role to a User Group, select the Role from the Members list and click . You can press **Ctrl** key for multiple selections.
 - To map all the Roles to a specific User Group, click .
 - To remove mapping for a user group, select the Role from Select Members list and click .
 - To remove all Roles mapped to a User Group, click .
4. Click **OK** to save the mappings and return to *UserGroup Role Map* screen.

3.7 System Administrator

3.7.1 Assumptions

- Administrator knows Database and SQL and can perform DML operations.
- The database schema will have proper privileges namely: **CONNECT, RESOURCE AND CREATE MATERIALIZED VIEW**, to execute the above mentioned scripts.
- Administrator knows how to start/shutdown the Web Application server.
- Administrator knows how to work on Oracle Financial Services Advanced Analytic Infrastructure.
- Depending on the access of the schedules for a given report, user can be created as:
 - View User
 - Analyst User
 - Authorize User
 - Super User

3.7.2 Pre-Requisites

- Simple Mail Transfer Protocol (SMTP) is already installed and configured on the Web Application Server and Access Control List (ACL) is created and assigned to the atomic schema designated for Information Domain where Oracle Financial Services Basel Regulatory Capital Release 8 is going to be installed. If not, SMTP needs to be installed and configured for Mailing Utility for the Reports following the Workflows. ACL creation and assigning to the Atomic Schema is mentioned in [Section 2.2.4](#).
- Administrator should also have access to Unified Metadata Manager in order to access Business Metadata Management -> Map Maintenance for creating a Mapper List used in Workflow Mail Utility.
- For accessing **Electronic Submission** under **Basel Regulatory Capital Analytics**, user or user groups should be mapped to FFIEC function. For more information, refer OFSAAI Installation & Configuration manual.
- Appropriate permission should be provided to Database Server for sending E-Mails.

3.7.3 Installing and Configuring SMTP on Web Application Server

SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection. An SMTP session consists of commands originated by an SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) so that the session is opened, and session parameters are exchanged

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) or a proprietary system (such as Microsoft Exchange or Lotus Notes/Domino) to access their mail box accounts on a mail server.

For more details regarding the Configuring SMTP servers, see http://docs.oracle.com/cd/B25553_01/mail.1012/b25499/servers_procs.htm

The Web Application Server should have access to the SMTP Server at the designated port for E-Mail Notification.

3.7.4 Creating a New Access Control List

3.7.4.1 Introduction

Secure authorization requires defining which users, applications, or functions can have access to which data, to perform which kinds of operations. Hence, there are three dimensions:

- (1) Which users can
- (2) Perform which operations
- (3) On which data.

We speak of (1) principals, (2) privileges, and (3) objects, corresponding to these three dimensions, respectively. Principals are users or roles.

Principals and privileges (dimensions 1 and 2) are related in a declarative way by defining access control lists. These are then related to the third dimension, data, in various ways, either declaratively or procedurally. For example, you can protect an Oracle XML DB Repository resource or table data by using PL/SQL procedure `DBMS_XDB.setACL` to set its controlling ACL.

3.7.4.2 Access Control Entry (ACE)

An access control entry (ACE) is an XML element (`ace`) that is an entry in an access control list (ACL). An ACE either grants or denies access to some repository resource or other database data by a particular principal (user or role). The ACE does not, itself, specify which data to protect. This is done outside the ACE and the ACL, by associating the ACL with target data. One way to make that association is by using PL/SQL procedure `DBMS_XDB.setACL`.

For more details, see

http://docs.oracle.com/cd/B28359_01/appdev.111/b28369/xdm21sec.htm

3.7.4.3 Access Control List (ACL)

An access control list (ACL) is a list of access control entries (ACEs). An access control list (ACL) has a single security class as its type. An ACL grants privileges to principals, to control access to protected data or functionalities. It can grant only the privileges that are defined in its security class. An ACL declares its security class with element `security-class`. If no such element is present in an ACL, then its type is the default security class, `DAV::dav`, which defines system privileges. Different ACLs can have as their type the same security class.

User has to mandatorily login with SYS user to create the ACL.

3.7.4.4 Creating new ACL

BEGIN

```
DBMS_NETWORK_ACL_ADMIN.create_acl (
  acl      => '<ffiec_acl_basel61dev.xml>',
  description => 'ACL for Electronic Submission ',
  principal => 'BASEL61DEV',
  is_grant  => TRUE,
  privilege  => 'connect',
  start_date => SYSTIMESTAMP,
  end_date  => NULL);
```

```
COMMIT;
END;
```

NOTE: User can provide an appropriate name for ACL Creation.

NOTE: User should provide the correct Principal name. The Principal (database user or role) name to whom the privilege is granted or denied are case sensitive.

For more information on ACL, refer to

http://docs.oracle.com/cd/B28359_01/appdev.111/b28419/d_networkacl_adm.htm

3.7.4.5 Assigning a network host to the ACL

BEGIN

```
DBMS_NETWORK_ACL_ADMIN.assign_acl (
  acl => '<ffiec_acl_basel61dev.xml>',
  host => TENY-ATRY-AXYD.oracle.com,
  lower_port => 1,
  upper_port => 1024);
```

```
END;
```

NOTE: User can provide an appropriate name for ACL Creation.

User should provide the host name to which ACL will be assigned. The host can be the name or the IP address of the host. A wildcard can be used to specify a domain or an IP subnet. The host or domain name is not case-sensitive. The sample name used is 'TENY-ATRY-AXYD.oracle.com'. User should provide the Lower bound of the TCP port range if not NULL. User should provide the Upper bound of the TCP port range. If NULL, the lower port is assumed.

3.7.4.6 Adding privilege to ACL

BEGIN

```
DBMS_NETWORK_ACL_ADMIN.ADD_PRIVILEGE(
  acl => 'ffiec_acl_basel61dev.xml',
  principal => 'BASEL61DEV',
  is_grant => TRUE,
  privilege => 'connect');
```

END;

3.7.5 Access of Web Application Server to SMTP server

The Web Application Server where the Basel Solution is installed should have access to the SMTP server at the designated port.

3.7.5.1 Updating Configuration table in Config Schema

Example value for MAILUTILITY_PDFHEADER = 'Oracle Financial Services Electronic Submission'

Example value for MAILUTILITY_PDFPATH = /tmp/summary.pdf

Example value for MAILUTILITY_SLEEPINTERVAL = 40000

Example value for MAILUTILITY_STATUS = 'Yes'

Example value for REV_MAIL_FROM = <BaselAdmin@oracle.com>

Example value for REV_SMTP_HOST = '<smtp host server>'

Example value for REV_SMTP_PORT = <port number>

Example value for <INFODOM>_<SEGMENT>_MASKING_PRIORITY_KEY = HREF0023

Example value for <INFODOM>_<SEGMENT>_ROLE_HIER = HREF0023

3.7.6 Data Preparation for Mail Utility

Mail Notification in OFS Electronic Submission is configured by providing data in WFM's tables in Atomic Schema.

The system admin has two options for Data Preparation for mail notification. They are:

- [Data Preparation for Role Notification using Workflow Current Stage](#)
- [Data Preparation for User Role Notification using custom data for Workflow](#)

3.7.6.1 Data preparation for Role Notification using Workflow Current Stage

This notification is initiated if the notification process is desired before/after achieving the required state of Workflow stage. This is initiated through a procedure

BASEL_FFIEC_NOTIFICATION which is entered in the Post condition of the Stage. This entry is made in WFM_STAGE_DETAILS.

Say the record status is 3, that is, Draft state and workflow is initiated to reach the next stage of Workflow. Then after the Workflow is completed, the Post condition is called using procedure BASEL_FFIEC_NOTIFICATION for notifying the user roles. Fetch the current stage of the workflow for the given record. Now depending on the User Access Method, either the user roles are fetched for the given stage from WFM_STAGE_ROLES or Users are fetched using the ROLE_USRGROUP_MAP and USER_GROUP_MAP which are mapped to the same User Group and Role.

3.7.6.2 Data preparation for User Role Notification using custom data for Workflow

This notification is initiated if there is entry present in WFM_NOTIFICATION_DETAILS for a given stage in WFM_STAGE_DETAILS. Depending on the current stage of workflow, the notify key are fetched. For the given notify key, the rules are applied and only those roles are notified who have passed the rule condition for a given stage of the workflow. The notify key - rules mapping is stored in WFM_STG_NOTIF_RULE_MAP. Now depending on the User Access Method, either the user roles are fetched for the given stage from WFM_NOTIFY_ROLES or Users are fetched using the ROLE_USRGROUP_MAP and USER_GROUP_MAP which are mapped to the same User Group and Role.

Note:

- **Default Email Utility is already configured based on the User - User Group - Role Mapping done through AAI - Administration - Security Management Screen.**
 - **An e-mail notification is configured for Super User roles to notify Super Users as soon as the Report is authorized. This is done in order to proceed with the Text File Generation.**
-

3.7.6.3 List of Seeded Tables and Setup Tables used in Workflow

List of tables which must be seeded in Workflow are:

1. WFM_LIST
2. WFM_MASTER
3. DIM_STATUS
4. DIM_STATUS_MLS
5. WFM_NOTIFICATION_DETAILS
6. WFM_RULE_DETAILS
7. WFM_STAGE_DETAILS

8. WFM_NOTIF_ROLES
9. WFM_STAGE_ROLES
10. WFM_STG_NOTIF_RULE_MAP
11. WFM_STG_ROUTE_RULE_MAP
12. WFM_STAGE_RULE_ROLES
13. WFM_STAGE_RULE_ROLES
14. FCT_BASEL_EMAIL_MAINTENANCE
15. DIM_USER_OPTIONS
16. DIM_PARENT_MODE
17. DIM_MASKING_RIGHTS
18. MASKING_VIEW_FFIEC
19. MASKING_VIEW_ES
20. FSI_SETUP_FORMS
21. FSI_SETUP_SCHEDULE_DETAILS
22. FSI_SETUP_EDIT_CHECKS

List of tables which must be setup in Workflow are:

1. WFM_NOTIF_USERS
2. WFM_STAGE_USERS
3. DIM_USER_OPTIONS
4. DIM_BASEL_CONFIGURATION
5. ROLE_USRGROUP_MAP

List of Intermediate Tables are:

1. WFM_ENTITY_STAGE_DTL

List of Output Tables are:

1. FCT_FFIEC_MAIL_AUDIT_STATUS
2. MAIL_AUDIT_TRAIL
3. ERROR_LOG_FFIEC

3.7.6.4 SEEDED TABLES

The Tables for Workflow and Mail Notification along with the Data are explained below:

1. **WFM_LIST:** This table defines the Workflow function mapped to different Entity Type. There can be only one workflow mapped to one entity.

N_WFM_LIST_ID	99
V_DSN_ID	BSL61BI
V_SEGMENT_ID	USABI
N_WFM_FN_ID	99
V_WFM_FN_NAME	FFIEC Reports Schedules
N_KBD_1_REQD	1
N_KBD_2_REQD	1
N_KBD_3_REQD	2
N_KBD_4_REQD	2
V_KBD_1_LABEL	Business Line
V_KBD_2_LABEL	Location
V_KBD_3_LABEL	
V_KBD_4_LABEL	
V_KBD_QUERY	
V_COMMENTS	
V_CREATED_BY	SHAILESH
D_CREATED_DATE	4/11/2013
V_LAST_MODIFIED_BY	
D_LAST_MODIFIED_DATE	

2. **WFM_MASTER:** This is the master table for Workflow function where the definition of the workflow is entered.

N_WFM_MASTER_ID	81258179
N_WFM_LIST_ID	99
N_WFM_VERSION	1
V_WFM_SHORT_NAME	Basel FFIEC Workflow for Schedule Level
V_WFM_DESC	Basel FFIEC Workflow for Schedule Level
N_KBD1_KEY	1
N_KBD2_KEY	1000
N_KBD3_KEY	1
N_KBD4_KEY	1
N_STATUS_KEY	50
V_COMMENTS	Basel FFIEC Workflow for Schedule Level
V_CREATED_BY	SHAILESH
D_CREATED_DATE	4/4/2013 18:39
V_LAST_MODIFIED_BY	
D_LAST_MODIFIED_DATE	
D_WFM_EFFECTIVE_DATE	4/4/2013
V_DEFAULT_WF_FLAG	Y

3. **DIM_STATUS:** This is master table for Status which is used in Electronic Submission Workflow. The Status Code, Key and Description are stored and are part of seeded data. Sample data for this table is given below:

N_STATUS_KEY	4
V_STATUS_NAME	New
V_STATUS_DESC	New
N_STATUS_CODE	4
F_LATEST_RECORD_INDICATOR	
D_RECORD_START_DATE	7/19/2011
D_RECORD_END_DATE	12/31/9999
V_MAKER_ID	
V_MAKER_REMARKS	
V_CHECKER_ID	
V_CHECKER_REMARKS	
D_MAKER_DATE	
D_CHECKER_DATE	
F_AUTHFLAG	
FIC_MIS_DATE	

4. **DIM_STATUS_MLS:** This table stores the Status description according to the Locale ID. The sample data for en_US locale is given below:

V_LOCALE_ID	en_US
N_STATUS_KEY	4
V_STATUS_NAME	New

5. **WFM_NOTIFICATION_DETAILS:** This table stores the notification keys depending on the Stage of the Workflow of the Schedule or the Quality Edit and the sequence of the notification to be sent.
- i. N_NOTIFY_KEY: Notification Key for a given stage and workflow master ID
 - ii. N_WFM_MASTER_ID: This column stores the Workflow Master ID
 - iii. N_NOTIF_STG_STATUS_KEY: This column stores the Status of the Stage of the Workflow.
 - iv. N_WF_NOTIF_SEQ: This column stores the sequence of the notification at any particular stage.
 - v. V_NOTIF_NAME: This column stores the name of the notification at any stage.
 - vi. V_NOTIF_DESC: This column stores the description for the notification created at any stage.

The Sample Data for this table is as follows:

N_NOTIF_KEY	N_WFM_MASTER_ID	N_NOTIF_STG_STAT_US_KEY	N_WF_NOTIF_SEQ	V_NOTIF_NAME	V_NOTIF_DESC
5000	81258179	3	1	Notify to Analyst on Editing any Report	Notify to Analyst on Editing any Report
5001	81258179	3	2	Notify to Authorizer on Editing any Report	Notify to Authorizer on Editing any Report
5002	81258179	7	1	Notify to Analyst on Submitting any Report for Approval	Notify to Analyst on Submitting any Report for Approval
5003	81258179	7	2	Notify to Authorizer for Report Pending for Approval	Notify to Authorizer for Report Pending for Approval
5004	81258179	8	1	Notify to Authorizer Group	Notify to Authorizer Group
5005	81258179	8	2	Notify to Analyst Group	Notify to Analyst Group

6. **WFM_RULE_DETAILS:** This table stores the rules of the workflow which decides the next stage of the workflow depending on the Pass or Fail of the rule condition at each stage.
- i. N_WFM_RULE_ID: This column stores workflow rule ID and is a running number for each rule definition.
 - ii. N_WFM_FN_ID: This column stores the Workflow function ID on which the rule has to be applied.
 - iii. V_RULE_NAME: This column stores the Workflow Rule Name for a given Workflow function ID.
 - iv. N_RULE_TYPE: This column stores the Workflow Rule Type for the defined Rule.

- v. V_RULE_DESC: This column stores the Workflow Rule Description of the defined Rule.
- vi. V_RULE_QUERY: This column stores the Workflow Rule Query. If the rule query successfully passes the criteria then the next stage of the Workflow is called. This stage rule mapping is defined in table WFM_STG_ROUTE_RULE_MAP.

The Sample Data for this table is as follows:

N_WFM_RULE_ID	81258075
V_DSN_ID	BSL61BI
V_SEGMENT_ID	USABI
N_WFM_FN_ID	99
V_RULE_NAME	Schedule Reports from New to Draft
N_RULE_TYPE	1
V_RULE_DESC	Schedule Reports from New to Draft
V_RULE_QUERY	DEFAULT
V_NOTES	
N_RULE_STATUS	1
V_COMMENTS	
V_CREATED_BY	SHAILESH
D_CREATED_DATE	3/27/2012
V_LAST_MODIFIED_BY	SHAILESH
D_LAST_MODIFIED_DATE	6/6/2012
N_RULE_PARAMETER_1	
N_RULE_PARAMETER_2	
N_RULE_PARAMETER_3	
N_RULE_PARAMETER_4	
N_RULE_PARAMETER_5	
D_RULE_PARAMETER_1	
D_RULE_PARAMETER_2	
V_RULE_PARAMETER	

- 7. **WFM_STAGE_DETAILS:** This table stores the data of the stages of the Workflow used in Electronic Submission. The Stages are defined along with the Stage Status keys to distinguish according to the stage of the record and sequence for the occurrence of the stages.
 - i. N_WFM_STAGE_ID: This column stores the different stage IDs of the Workflow for a given Workflow Function
 - ii. N_WFM_MASTER_ID: This column stores the Workflow Function ID for which the stages defined.
 - iii. N_STAGE_SEQ_ID: This column stores the sequences of the Workflow Stages.
 - iv. N_STAGE_LVL_SEQ_ID: This column stores the sequence of the sub stages with the Workflow Stages.

- v. N_WFM_STAGE_STATUS_KEY: This column stores the status of the stages of the Workflow. This status corresponds to the record status to identify it stage.
- vi. V_STAGE_NAME: This column stores the Workflow Stage names.
- vii. V_STAGE_DESC: This column stores the Workflow Stage description.
- viii. N_STAGE_MANDATORY_IND: This column stores the data to identify the mandatory stages of the workflow. 1 is represented as mandatory stage and 2 is represented as non mandatory stage and the stage can be skipped in workflow to follow the next stage.
- ix. N_USER_ACCESS_METHOD: This column stores the approach to be followed while notifying the users at the beginning or end of any stage. If N_USER_ACCESS_METHOD is 1 or 2, then the roles of the stages are fetched and for each role, if the rule condition is satisfied then the users are fetched for notification. If N_USER_ACCESS_METHOD is 3, then the all the roles are fetched for each stages and then the users based on User Role mapping in Config Schema are fetched for notification.
- x. V_WFM_PRECON: This stores the precondition procedure names (comma separated) which needs to be called at the starting of any stage if specified.
- xi. V_WFM_POSTCON: This stores the post condition procedure names (comma separated) which needs to be called at the completion of any stage if specified.

N_WFM_STAGE_ID	81258185
N_WFM_MASTER_ID	81258179
N_STAGE_SEQ_ID	2
N_STAGE_LVL_SEQ_ID	2
N_WFM_STAGE_STATUS_KEY	3
V_STAGE_NAME	Draft
V_STAGE_DESC	Upload Reports after Edit is in Draft status.
N_STAGE_MANDATORY_IND	2
N_STAGE_OPTIONS	1
N_USER_ACCESS_METHOD	1
V_COMMENTS	
V_WFM_PRECON	
V_WFM_POSTCON	BASEL_FFIEC_NOTIFICATION, BASEL_FFIEC_NOTIFICATION_WFM, PR_FFIEC_UPD_SCHEDULE_STATUS

N_WFM_STAGE_ID	81258180
N_WFM_MASTER_ID	81258179
N_STAGE_SEQ_ID	1
N_STAGE_LVL_SEQ_ID	1
N_WFM_STAGE_STATUS_KEY	4
V_STAGE_NAME	New
V_STAGE_DESC	Uploaded Report has a New Status
N_STAGE_MANDATORY_IND	1
N_STAGE_OPTIONS	1
N_USER_ACCESS_METHOD	1
V_COMMENTS	
V_WFM_PRECON	
V_WFM_POSTCON	PR_FFIEC_UPD_SCHEDULE_STATUS

8. **WFM_NOTIF_ROLES:** This table stores the roles to be notified after / before the stage is achieved either through Precondition procedure or Post condition procedure.
- i. N_NOTIF_ROLE_KEY: This column stores the notification role key for a given notification key and User role.
 - ii. N_NOTIF_KEY: This column stores notification key for a given stage and workflow master ID.
 - iii. V_USER_ROLE_CODE: This column stores the role information for notification for a given notification key.
 - iv. V_COMMENTS: This column stores the comments for the notification role key.
 - v. N_NOTIF_ROLE_STATUS: This column stores the flag for the roles for which notification is applicable.

	N_NOTIF_ROLE_KEY	N_NOTIF_KEY	V_USER_ROLE_CODE	V_COMMENTS	N_NOTIF_ROLE_STATUS
1	5002	5000	AVIEWER	Schedule A View Role	1
2	5003	5000	AANALYST	Schedule A Analyst Role	1
3	5004	5001	AAUTHORIZE	Schedule A Auth Role	1
4	5005	5000	ASUPERUSR	Schedule A SuperUsr Role	1
5	5006	5000	BANALYST	Schedule B Analyst Role	1
6	5007	5001	BAUTHORIZE	Schedule B Auth Role	1
7	5008	5000	BSUPERUSR	Schedule B SuperUsr Role	1

9. **WFM_STAGE_ROLES**: This table stores the data for the Role which is mapped to the stages of the Workflow.

- i. **N_STAGE_ROLE_KEY**: This column stores the stage role key for a given stage and role.
- ii. **N_WFM_STAGE_ID**: This column stores the workflow stage key.
- iii. **N_USER_ROLE_CODE**: This column stores the User Role code for a given Workflow stage key.
- iv. **N_STAGE_ROLE_STATUS**: This column stores the flag for the stage – role combination which needs to be notified or restricted.
- v. **V_COMMENTS**: This column stores the description of the record created for stage – role combination.

	N_STAGE_ROLE_KEY	N_WFM_STAGE_ID	V_USER_ROLE_CODE	N_STAGE_ROLE_STATUS	V_COMMENTS
1	1	81258180	AVIEWER	1	Viewer Role for Schedule A
2	2	81258180	BVIEWER	1	Viewer Role for Schedule B
3	3	81258180	CVIEWER	1	Viewer Role for Schedule C
4	41	81258190	AAUTHORIZE	1	Authorizer Role for Schedule
5	42	81258190	BAUTHORIZE	1	Authorizer Role for Schedule

10. **WFM_STAGE_RULE_ROLES**: This table stores the rules mapped to each stage role key combination. These are uniquely identified by N_RULE_ROLE_KEY.

- i. **N_RULE_ROLE_KEY**: This column stores the unique identifier for rule and stage – role key combination.
- ii. **N_WFM_RULE_ID**: This column stores the rule id mapped to stage – role key combination. The details of the rules are defined in WFM_RULE_DETAILS tables.
- iii. **N_STAGE_ROLE_KEY**: This column stores the stage role keys on which rules are applicable. The definitions are stored in WFM_STAGE_ROLES table.
- iv. **N_STG_RULE_ROLE_STATUS**: This column stores the flag for the record for which needs to be notified at achieving this stage.
- v. **V_COMMENTS**: This column stores the comments of the record.

	N_RULE_ROLE_KEY	N_WFM_RULE_ID	N_STAGE_ROLE_KEY	N_STG_RULE_ROLE_STATUS	V_COMMENTS
1	1	81258076	21	1	Report in Pending Approval State
2	2	81258076	22	1	Report in Pending Approval State
3	3	81258076	23	1	Report in Pending Approval State
4	40	81258076	60	1	Report in Approved State
5	41	81258076	61	1	Report in Approved State
6	42	81258076	62	1	Report in Approved State

11. **WFM_STG_NOTIF_RULE_MAP**: This table stores the mapping of the Notification Key and Rule ID to be applied. These are uniquely identified by N_NOTIF_RULE_MAP_ID.

- i. N_NOTIF_RULE_MAP_ID: This column stores the unique identifier for notification key and rule mapping.
- ii. N_NOTIF_KEY: This column stores the notification key for which rule needs to be applied.
- iii. N_WFM_RULE_ID: This column stores the rule ID which is mapped to the notification key.
- iv. N_RULE_MAP_STATUS: This column stores the flag for the record for which the rule needs to be applied for a given notification key.
- v. V_COMMENTS: This column stores the comments of the record.

	N_NOTIF_RULE_MAP_ID	N_NOTIF_KEY	N_WFM_RULE_ID	N_RULE_SEQ	N_RULE_MAP_STATUS	V_COMMENTS
1	81257514	5000	81258076	1	1	
2	81257515	5001	81258076	1	1	
3	81257516	5002	81258076	1	1	
4	81257517	5003	81258076	1	1	
5	81257518	5004	81258076	1	1	

12. **WFM_STG_ROUTE_RULE_MAP**: This table stores the stage rule map id which decides the next stage of the workflow to be followed on passing the rule id for a current stage. These are uniquely identified by N_STAGE_RULE_MAP_ID.

- i. N_STAGE_RULE_MAP_ID: This column stores the unique identifier for stage routing rule map keys.
- ii. N_WFM_STAGE_ID: This column stores the current stage of the workflow.
- iii. N_WFM_RULE_ID: This column stores the rule ID which needs to be applied for moving to the next stage mapped to it.
- iv. N_RULE_SEQ: This column stores the sequence of the rules to be applied at the current stages. If the first rule fails, then the sequence decides the next rule to be applied.
- v. N_NXT_STAGE_ID: This column stores the next level stage ID which the workflow will move into after executing the pre condition
- vi. N_RULE_MAP_STATUS: This column stores the flag for the record for which the stage route rule map needs to be applied.

	N_STAGE_RULE_MAP_ID	N_WFM_STAGE_ID	N_WFM_RULE_ID	N_RULE_SEQ	N_NXT_STAGE_ID	N_RULE_MAP_STATUS	V_COMMENTS
1	81259013	81258180	-1	1	81258185	1	
2	81259014	81258185	-1	1	81258190	1	
3	81259015	81258190	81258078	1	81258185	1	
4	81259016	81258190	81258077	2	81258195	1	

13. **FCT_BASEL_EMAIL_MAINTENANCE**: This table stores the Role Code and Mail Body Mapping. The Mail Header and the Body is selected based on the Role Code of the User mapped, status of the Record and the Authorization and Rejection flag of the record.

The sample data for this table is as follows:

V_ROLE_CODE	KAUTHORIZE
N_EMAIL_MAIN_KEY	47
V_MSG_DESC	hii
V_MSG_SUBJECT	[SCHEDULENAME] - [REPORTNAME] - Rejected
V_MSG_BODY	Hi [USERID],
N_ENTITY_KEY	99
N_WF_ACTIONTYPE_KEY	7
V_WF_ACTIONFLAG	R

14. **WFM_STAGE_RULE_ROLES**: This table stores the Role – Rule mapping. Each mapping is stored with unique N_RULE_ROLE_KEY. The Rule definitions are stored in WFM_RULE_DETAILS. The sample data for this table is as follows:

N_RULE_ROLE_KEY	N_WFM_RULE_ID	N_STAGE_ROLE_KEY	N_STG_RULE_ROLE_STATUS	V_COMMENTS
21	81258076	41	1	Report in Pending Approval State
22	81258076	42	1	Report in Pending Approval State
23	81258076	43	1	Report in Pending Approval State

15. **DIM_PARENT_MODE**: This table stores the data for Parent Mode which is used in Masking. It has only two entries VIEW and EDIT with its corresponding identifier keys.
16. **DIM_MASKING_RIGHTS**: This table stores the data for action for masking. Depending on the action and various parameters like record, status, parent mode and so on the grid masking is configured. The following is the Sample Data for the DIM_MASKING_RIGHT.

N_MASKING_RIGHT_KEY	V_MASKING_RIGHTS_NAME
1	VIEW
2	EDIT
3	CREATENEW
4	DELETE
5	CLOSE
7	EXPORT
8	ASSESSMENT
9	ATTESTATION
10	GENERATETEXT
11	AUTHORIZE
12	AUTHSCHD
13	AUTHCOMMENTS
14	RESET
15	GENEDITCHECKS
16	VIEWTXT

17. **MASKING_VIEW_FFIEC**: This table stores the data for Summary Page Grid Masking. The buttons on the header of the grid will be disabled by default except Upload button. On selecting any report, the buttons on the grid gets enabled depending on the Masking Right, Report Status, Parent Mode, Parent Status and Role of the User logged-in.

Though the data is seeded, the same can be configured using Map Maintenance under **Home -> Unified Metadata Manager -> Business Metadata Management -> Map Maintenance**. Please refer to OFSAAI Installation and Configuration manual for more details.

The Sample Data for the Masking_View_FFIEC table is as follows:

VERSION_NO	1
LOCALE	en_US
HREF035	AUTHSCHD
UK_HREF035	[HREF035].[AUTHSCHD]
HREF035_DESC	AUTHSCHD
HREF035_LEVEL	LEVEL0
HREF034	2
UK_HREF034	[HREF034].[2]
HREF034_DESC	EDIT
HREF034_LEVEL	LEVEL0
HRES01	13
UK_HRES01	[13]
HRES01_DESC	Open
HRES01_LEVEL	LEVEL0
HREF0023	ECAUTHORIZ
UK_HREF0023	[HREF0023].[ECAUTHORIZ]
HREF0023_DESC	Role for Authorizer Edit Checks
HREF0023_LEVEL	LEVEL0
HRES02	50
UK_HRES02	[HRES02].[50]
HRES02_DESC	Active
HRES02_LEVEL	LEVEL0

18. **MASKING_VIEW_ES**: This table stores the data for Schedule Grid Masking. The button on the Grid i.e. View, Edit, Authorize and Reset enables depending on the Role of the logged-in User, Schedule selected, Parent Mode, Parent Status, Schedule Status and Masking Action.

Though the data is seeded, the same can be configured using Map Maintenance under **Home → Unified Metadata Manager → Business Metadata Management → Map Maintenance**. Please refer to OFSAAI Installation and Configuration manual for more details.

The Sample Data for this table is given below:

VERSION_NO	1
LOCALE	en_US
HREF0023	RANALYST
UK_HREF0023	[HREF0023].[RANALYST]
HREF0023_DESC	Schedule R Analyst Role
HREF0023_LEVEL	LEVEL0
HREF034	2
UK_HREF034	[HREF034].[2]
HREF034_DESC	EDIT
HREF034_LEVEL	LEVEL0
HRES01	13
UK_HRES01	[HRES01].[13]
HRES01_DESC	New
HRES01_LEVEL	LEVEL0
HREF101	20
UK_HREF101	[HREF101].[20]
HREF101_DESC	Sheet Name for Call31 RC
HREF101_LEVEL	LEVEL0
HRES02	72
UK_HRES02	[HRES02].[72]
HRES02_DESC	New
HRES02_LEVEL	LEVEL0
HREF035	VIEW
UK_HREF035	[HREF035].[VIEW]
HREF035_DESC	VIEW
HREF035_LEVEL	LEVEL0

19. **FSI_SETUP_FORMS**: This table stores the Data for the Schedules name used in FFIEC and Non FFIEC Report along with the corresponding form ID , sheet key, sheet description and flag for schedule or not.

The sample data for this table is as follows:

V_SHEET_NAME	V_FORM_ID	N_SHEET_SKEY	V_SHEET_DESC	ISSCHEDULE
Schedule A	frmSchAParent	1	Sheet Name for Schedule A	Y
Schedule B	frmSchBParent	2	Sheet Name for Schedule B	Y
Schedule C	frmTestParent	3	Sheet Name for Schedule C	Y
Schedule D	frmSchDParent	4	Sheet Name for Schedule D	Y
Schedule E	frmSchEParent	5	Sheet Name for Schedule E	Y
Schedule F	frmSchFParent	6	Sheet Name for Schedule F	Y
Schedule G	frmSchGParent	7	Sheet Name for Schedule G	Y
Schedule H	frmSchHParent	8	Sheet Name for Schedule H	Y
Schedule I	frmSchIParent	9	Sheet Name for Schedule I	Y
Schedule J	frmSchJParent	10	Sheet Name for Schedule J	Y
Schedule K	frmSchKParent	11	Sheet Name for Schedule K	Y
Schedule L	frmSchLParent	12	Sheet Name for Schedule L	Y
Schedule M	frmSchMParent	13	Sheet Name for Schedule M	Y
Schedule N	frmSchNParent	14	Sheet Name for Schedule N	Y
Schedule O	frmSchOParent	15	Sheet Name for Schedule O	Y
Schedule P	frmSchPParent	16	Sheet Name for Schedule P	Y
Schedule Q	frmSchQParent	17	Sheet Name for Schedule Q	Y
Schedule R	frmSchRParent	18	Sheet Name for Schedule R	Y
Schedule S	frmSchSParent	19	Sheet Name for Schedule S	Y
CALL31_RC	frmCall31Parent	20	Sheet Name for Call31 RC	N
CALL31_RC_R	frmCall31RCRParent	21	Sheet Name for Call31 RCR	N
CALL41_RC	frmCall41Parent	22	Sheet Name for Call41 RC	N
CALL41_RC_R	frmCall41RCRParent	23	Sheet Name for Call41 RCR	N
FRY9C_HC	frmFRY9CParent	24	Sheet Name for FRY9C HC	N
FRY9C_HC_R	frmFRY9CHCRParent	25	Sheet Name for FRY9C HCR	N
Quality Checks, Inter-Series & Post Inter-Series Edit Checks	frmQualityParent	26	Sheet Name for Quality Checks, Inter-Series & Post Inter-Series Edit Checks	E
Validity Checks	frmValidityParent	27	Sheet Name for Validity Checks	E

20. **FSI_SETUP_SCHEDULE_DETAILS**: This table stores the details of the Schedules including the Line Identifier, Schedule Name, Row Number, and Line Order, Data type of the cell and flag for the cell to be disabled or not and whether it's dummy cells which are created explicitly for headers used in Grid.

The sample data for the table is as follows:

V_LINE_IDENTIFIER	LAAFCJ008
V_SCHEDULE_NAME	F
N_ROW_NUMBER	6
N_COLUMN_NUMBER	5
N_LINE_ORDER	28
V_DATATYPE	I
N_MIN_LENGTH	0
N_MAX_LENGTH	12
V_LINE_NO_DESC	2
F_IS_DUMMY	
F_IS_DISABLED	

21. **FSI_SETUP_EDIT_CHECKS**: This table stores the details of the Edit Checks like Form Number, Effective Start and End Date, Edit Type and many more parameters as follows.

V_COLUMN_NAME	V_REPORT_TYPE	N_READ_ORDER	N_WRITE_TO_TEXT_ORDER	V_DATATYPE	V_COLUMN_TYPE	V_PREFIX	V_VALUE_CHECK	N_DB_WRITE_ORDER
V_SERIES	Validity	1		T				12
FORM_NUMBER	Quality			I	VALUE			
N_EFFECTIVE_START_DATE	Validity	2		I				13
N_EFFECTIVE_END_DATE	Validity	3		I				14
V_TYPE_OF_CHANGE	Validity	4		T				15
V_PUBLICATION	Validity	5		T				16
V_SCHEDULE	Validity	6		I				
OCCURRENCE	Quality			I	VALUE			
V_SERIES	Quality	1	6	T	VALUE			12
N_EFFECTIVE_START_DATE	Quality	2	7	I	VALUE			13
N_EFFECTIVE_END_DATE	Quality	3	8	I	VALUE			14
V_TYPE_OF_CHANGE	Quality	4	9	T	VALUE			15
V_PUBLICATION	Quality	5	10	T	VALUE			16
V_SCHEDULE	Quality	6		I	VALUE			
V_EDIT_TYPE	Quality	7	2	I	VALUE			4
V_EDIT_NUMBER	Quality	8	1	I	VALUE	E		5
V_TARGET_ITEM	Quality	9		I	VALUE			6
V_MDRM_NO	Quality	10	3	I	VALUE			7
V_COMPARISON_SERIES	Quality	11	4	I	VALUE			8
V_EDIT_TEST	Quality	12		T	VALUE			9
V_RESULTS	Quality	13		T	COMPARATOR		OK,Not Applicable	10
V_edit_COMMENTS	Quality	14	5	T	VALUE			11
V_EDIT_TYPE	Validity	7		I				4
V_EDIT_NUMBER	Validity	8		I				5
V_EDIT_TEST	Validity	11		T				9
V_TARGET_ITEM	Validity	9		I				6
V_MDRM_NO	Validity	10		I				7
V_COMPARISON_SERIES	Validity	13		I				8
V_RESULTS	Validity	12		T				10
V_edit_COMMENTS	Validity	14		T				11

3.7.7 SETUP DATA

1. **WFM_NOTIF_USERS:** This table stores the Users to be notified after/ before the stage is achieved either through the Precondition procedure or Post condition procedure. The master table is WFM_NOTIF_ROLES which stores the Roles to be notified at a given Notification Key. The User corresponding to these roles are stored in WFM_NOTIF_USERS.
 - i. N_NOTIF_USER_KEY: This column stores the notification user key for a given notification key and User Id. Any Sequential number can be provided.
 - ii. N_NOTIF_ROLE_KEY: This column stores the notification role key for a given notification user key. Refer WFM_NOTIF_ROLES for appropriate notification role key.
 - iii. V_USER_ID: This column stores the User id for the Users to notify the event change after/before the Status change at a given stage.
 - iv. N_NOTIF_USER_STATUS: This column stores the flag for the Users who need the notification at stages. If value 1, then User is notified with the status changes if applicable.
 - v. V_COMMENTS: This column stores the comments of the record created for notifying the User.

	N_NOTIF_USER_KEY	N_NOTIF_ROLE_KEY	V_USER_ID	N_NOTIF_USER_STATUS	V_COMMENTS
1	1	5003	SACHIN	1	
2	2	5003	SHAILESH	1	
3	3	5004	SENTHIL	1	
4	4	5004	MAHALAKSHMI	1	
5	5	5005	SHOUGAT	1	

2. **WFM_STAGE_USERS**: This table stores the data for the Users which are mapped to the stage role key combination. The master table is WFM_STAGE_ROLES which stores role code - keys combination.

- i. N_STAGE_USER_KEY: This column stores the stage user key for a given role – user combination. Any sequential number can be provided.
- ii. N_STAGE_ROLE_KEY: This column stores the stage – role key which identifies the user to be notified based on this stage of the workflow. Refer WFM_STAGE_ROLES for appropriate stage role key combination.
- iii. V_USER_ID: This column stores the User ID of the Users which needs to be notified depending on the Stage – Role combination.
- iv. N_STAGE_USER_STATUS: This column stores the flag for the User who needs to be notified at achieving this stage.
- v. V_COMMENTS: This column stores the description of the record.

	N_STAGE_USER_KEY	N_STAGE_ROLE_KEY	V_USER_ID	N_STAGE_USER_STATUS	V_COMMENTS
1	1	41	SENTHIL	1	Authorizer for Schedule A should be informed
2	2	41	MAHALAKSHMI	1	Authorizer for Schedule A should be informed
3	3	41	SHOUGAT	1	Super User for Schedule A should be informed
4	4	42	SENTHIL	1	Authorizer for Schedule B should be informed
5	5	42	SHOUGAT	1	Super User for Schedule B should be informed
6	6	43	MUKUL	1	Authorizer for Schedule C should be informed

3. **DIM_USER_OPTIONS**: This table stores the data of the User IDs of the Users who want to be notified for any schedule or report changes. E-mail notification is only supported for this release. Here, N_EMAIL_REQ should be given as 0 if the given User agrees to receive Mail for the Workflow Process. If User wishes to opt out of Mailing Process, then N_EMAIL_REQ can be changed to 1.

The sample data for this table is as follows:

N_MAP_KEY	V_USER_ID	D_CREATED_DATE	V_CREATED_BY	V_LOCALE_ID	N_EMAIL_REQ
4	MUKUL	5/27/2013	SHAILESH	en_US	0
5	SACHIN	5/27/2013	SHAILESH	en_US	0
6	SENTHIL	5/27/2013	SHAILESH	en_US	0
7	SUGANDHA	5/27/2013	SHAILESH	en_US	0
8	SHAILESH	5/27/2013	SHAILESH	en_US	0
9	MAHALAKSHMI	5/27/2013	SHAILESH	en_US	0
10	SHOUGAT	5/27/2013	SHAILESH	en_US	0

4. **DIM_BASEL_CONFIGURATION:** This table stores the default locale used for Basel Solution and the administrator mail from whom the mail utility sends the mail. The following is the sample data for this table.

N_CONFIG_KEY	V_PARAMNAME	V_PARAMVALUE	V_DESCRIPTION
1	EMAIL_DEFAULT_LOCALE	en_US	Default locale for email notification
2	REV_MAIL_FROM	skchinna_directs_ww@oracle.com	Oracle Reveleus Mail from id

5. **ROLE_USRGROUP_MAP:** This mapping can be done only by those users, who have access to **Unified Metadata Manager** by using the **Map Maintenance Module** in **Oracle Financial Services Analytics Infrastructure**. The input to this module is a hierarchy HREF0023 which is created on a View USER_ROLE. This is based on CSSMS_ROLE_MAST in config schema and hierarchy HREF0024. This is created on a View USER_GROUP_MAST which is based on CSSMS_GROUP_MAST in config schema.

NOTE: Ensure that the hierarchies are available before proceeding to the Map Maintenance screen. User should resave the two hierarchies before creating new Mapper Definition (this is mandatory).

NOTE: Admin User must be mapped to Function “CRTMAPADV – Create Map Advanced” before creating the Mapping Definition (this is mandatory).

The following are the steps required to create Mapping Definition:

- i. Choose the Map Maintenance screen at Oracle Financial Services Analytics Infrastructure -> Unified Metadata Manager -> Business Metadata Management -> Map Maintenance.
- ii. Select the Segment Name corresponding to USA Segment.
- iii. Click Create New Map.
- iv. Enter the Description for Mapper Definition.
- v. Uncheck the Dynamic option.

- vi. Enter the Database Entity Name as `ROLE_USRGROUP_MAP`.

NOTE: Ensure that you do not provide any other name.

- vii. Provide the comments for the Mapper Definition. Comments to the New Entry can be left blank.
- viii. Select the hierarchies HREF0023 and HREF0024. The sample name given for these hierarchies are “User Role” and “User Group”. In case these two hierarchies are not appearing in the Member list on left pane, ensure that the hierarchies are mapped to the selected segment which can be done through System Configuration -> Segment/Metadata Mapping.
- ix. Click Save. A new Mapper is created in the Mapper List and the table `ROLE_USRGROUP_MAP` is created in the mapped Atomic Schema.
- x. Select this Mapper and click Mapper Maintenance. The two selected hierarchies are displayed along with the Data.
- xi. Select the nodes and then click Save Mapping.
- xii. Select the nodes and then click Save.
- xiii. The Administrator can map the User Role to the required User Groups. In case the Mapping needs to be deleted, Administrator can select the node for which the mapping needs to be deleted and then click Delete Mapping.
- xiv. Click View Mapping. It helps the Administrator to view the existing Mapping if any.
- xv. After the mapping is completed click Save.
- xvi. Click **Close** to close the screen.
- xvii. Administrator must verify the mapping entries in **`ROLE_USR_GROUP_MAP`** table.

NOTE: In case the Administrator does not setup the tables as mentioned above, the default configuration as done through Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) is picked up from the Config Schema. The corresponding User Role configuration will be used for notifying the Users for Mail Utility.

3.7.8 MASKING DATA PREPARATION

This section is meant only to provide information on Grid Masking and Control Masking and User intervention is not required.

NOTE: DO NOT modify Data in `MASKING_VIEW_FFIEC` and `MASKING_VIEW_ES`.

3.7.8.1 GRID MASKING DATA PREPARATION

Grid Level masking is generally applied on the tool bar on grid which needs to be enabled on selection of record. The enabling of the record depending on the various factors such as record name, role assigned to access that record, status of the record, parent mode and parent status which are passed through the parent form or click of any button or on page reload. The form will have the ACTIONRIGHT tag which will differentiate the actions accordingly. The functions used for masking are:

1. **Masking_Reports:** This function is used for masking the buttons on the tool bar in Report Level Grid. This grid is in the Summary Page Screen where the list of the reports is displayed. Initially all the buttons in the disabled state i.e. the renderer mode for button will be in disabled mode, 3 ,except the Upload Button as Upload button can be clicked with or without selecting the report from Report list screen.

When any record is selected, depending on the entry for the status of the record, parent mode, parent status and role of the logged in User in Masking_view_ffiec, the buttons are enabled.

Say for example, any report which is newly added to the Report List is in status Active (50), then the button such as View for Schedules, View/Download to view and download the excel format of the report, Edit Check for viewing the Quality, Inter Series and Validity Check can be viewed.

Masking Reports uses MASKING_VIEW_FFIEC entries for enabling the Data on selecting any grid record.

Sample Data for MASKING_VIEW_FFIEC is as follows.

VERSION_NO	1
LOCALE	en_US
HREF035	AUTHSCHD
UK_HREF035	[HREF035].[AUTHSCHD]
HREF035_DESC	AUTHSCHD
HREF035_LEVEL	LEVEL0
HREF034	2
UK_HREF034	[HREF034].[2]
HREF034_DESC	EDIT
HREF034_LEVEL	LEVEL0
HRES01	13
UK_HRES01	[13]
HRES01_DESC	Open
HRES01_LEVEL	LEVEL0
HREF0023	ECAUTHORIZ
UK_HREF0023	[HREF0023].[ECAUTHORIZ]

HREF0023_DESC	Role for Authorizer Edit Checks
HREF0023_LEVEL	LEVEL0
HRES02	50
UK_HRES02	[HRES02].[50]
HRES02_DESC	Active
HRES02_LEVEL	LEVEL0

2. **Masking_Reports_Schedule:** This function is used for masking the buttons on the tool bar in Schedule Level Grid. This grid is in Schedule List Screen where the list of the schedules is displayed. Initially all the buttons will be in disabled state, on selecting the schedule, depending on the entry made in Masking_view_es for status of the schedule, parent mode, parent status, record name, record status and the role of the logged-in User, the toolbar button will be enabled.

Say for example, select any schedule for a newly uploaded report is in status New (4), then the View button is enabled for the Users who are mapped to the Viewer Role for the selected Schedule. The Edit button will be only enabled if the User is having the Edit permission and the status is not pending for approval. The Authorize button is enabled only for the Users who are mapped to the Authorizer Role for the selected Schedule. The Reset button is enabled only for the Super User.

Masking_Reports_Schedule uses MASKING_VIEW_ES data for enabling Data on basis of Parent Mode, Parent Status, Record Status, Record Name and Role of the Record.

Sample Data is as follows.

VERSION_NO	1
LOCALE	en_US
HREF0023	RANALYST
UK_HREF0023	[HREF0023].[RANALYST]
HREF0023_DESC	Schedule R Analyst Role
HREF0023_LEVEL	LEVEL0
HREF034	2
UK_HREF034	[HREF034].[2]
HREF034_DESC	EDIT
HREF034_LEVEL	LEVEL0
HRES01	13
UK_HRES01	[HRES01].[13]
HRES01_DESC	New
HRES01_LEVEL	LEVEL0
HREF101	20

UK_HREF101	[HREF101].[20]
HREF101_DESC	Sheet Name for Call31 RC
HREF101_LEVEL	LEVEL0
HRES02	72
UK_HRES02	[HRES02].[72]
HRES02_DESC	New
HRES02_LEVEL	LEVEL0
HREF035	VIEW
UK_HREF035	[HREF035].[VIEW]
HREF035_DESC	VIEW
HREF035_LEVEL	LEVEL0

4 OFS Economic Capital Advanced Analytics Configuration

4.1 Assumptions

- The database schema will have proper privileges namely, CONNECT, RESOURCE AND CREATE MATERIALIZED VIEW.
- OBIEE 11.1.1.7.150120 (64-bit) server or higher for the respective operating system is installed
- Administrator knows how to start/shutdown the OBIEE servers namely;
 - WebLogic Server
 - Oracle BI Server
 - Oracle BI Presentation Server
 - Oracle BI Java Host
- Administrator knows the OBIEE installation path

4.2 Prerequisites

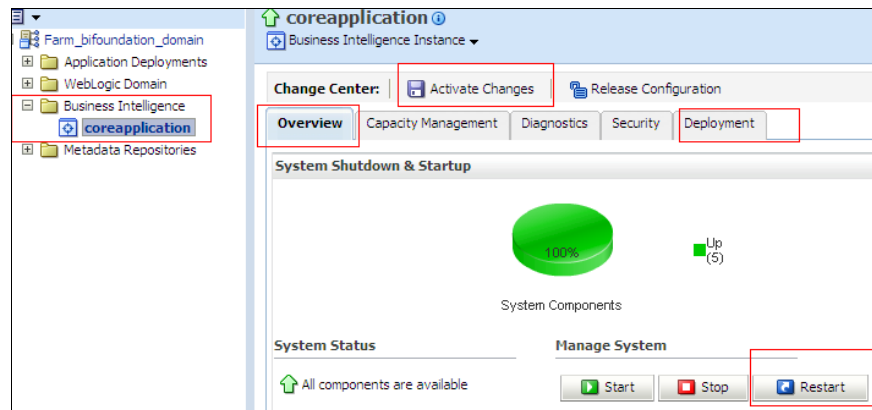
- a. Backup the following OBIEE folders (*This is recommended only for existing installation. It is not required for new installation.*) :
 - `<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIServerComponent\coreapplication_obis1\repository`
 - `<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog\<new folder created as part of Installation steps>`
- b. Server details that is, the URL of OBIEE must be kept ready.
- c. Copy the following files from the release kit to the local system:
 - `$FIC_HOME/CAP/catalog/CREC/OFS Economic Capital Advanced - Answers`; this has the archive for Answer (report) related files. Do not unzip this file, as this file is not a zip file.
 - `$FIC_HOME/CAP/catalog/CREC/OFS Economic Capital Advanced-Dashboards`; this has the archive for Dashboard related files. Do not unzip this file, as this file is not a zip file.
 - `$FIC_HOME/CAP/repository/OFS Economic Capital Advanced-repository.zip`; this has the rpd file. Unzip this file in the local machine.

4.3 Configuration Steps

4.3.1 Server Configuration Steps

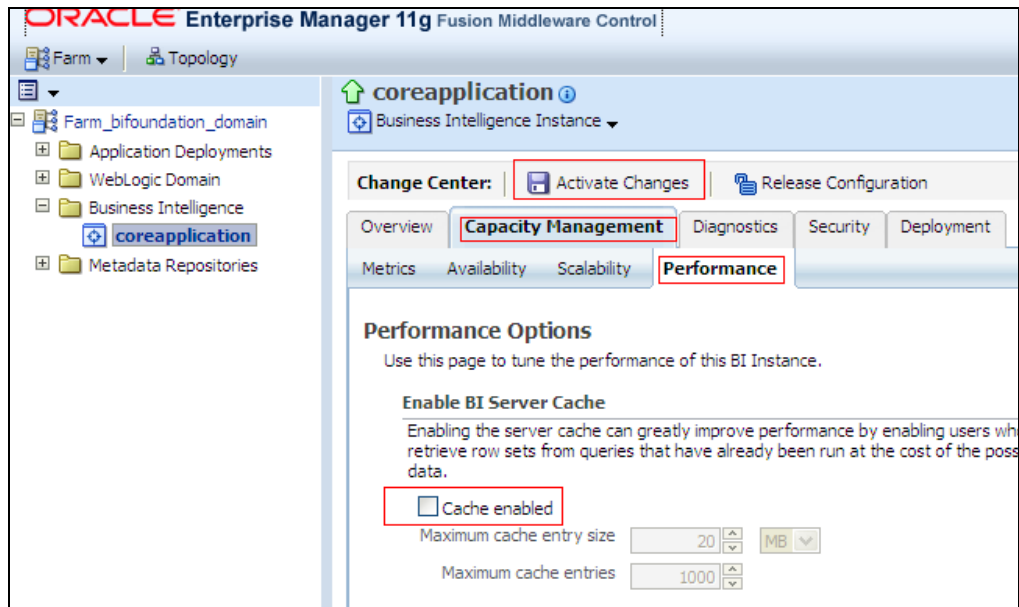
For each release, perform the following instructions for the server setup:

- a. Stop the BI servers
 - ii. Go to Business Intelligence menu located on the left hand side of the screen and then select **core application**.
 - iii. Click **Deployment** tab.
 - iv. Click **Lock and Edit Configuration**.
 - v. Go to the section Upload BI Repository and browse to select the repository.
 - vi. Enter the repository password and confirm the same. The repository password is “Administrator1”.
 - vii. Click **Apply**.
 - viii. Go to BI Presentation Catalog section and then provide the path of the new catalog.
 - ix. Click **Activate Changes**.
 - x. Click **Overview** tab.
 - xi. Click **Restart** and confirm to restart all services.

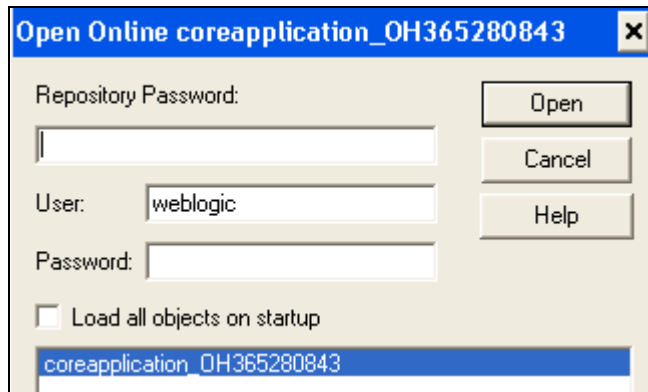


- xii. Edit the **NQSConfig.INI** file, present in *<Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1* to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = NO to YES.
- xiii. Add the following tag: `<UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs>` in the instanceconfig.xml under the tag `<Catalog>`, present in *<Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent* and restart all opmn services.

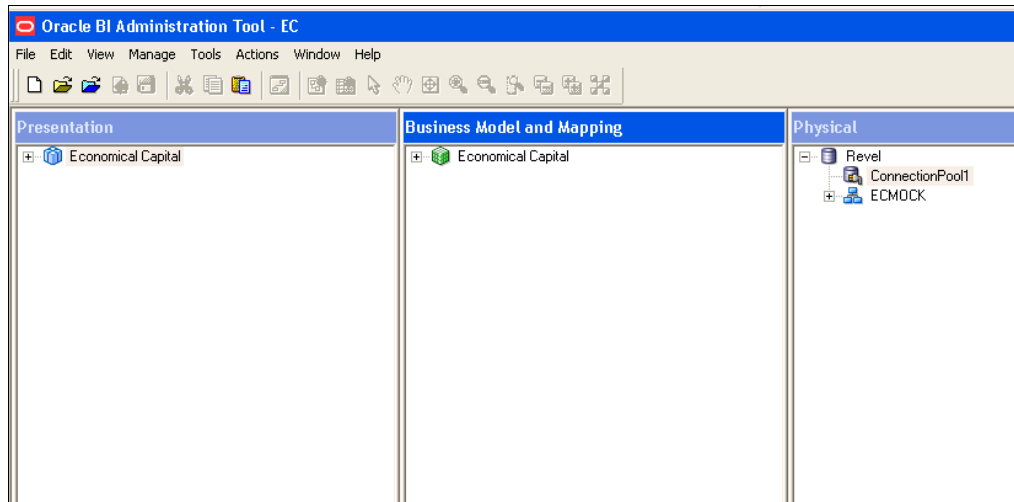
- xiv. Check if all the servers are up and running (except Presentation Service).
- xv. Edit the NQSConfig.INI file, present in <Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1 to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES to NO and update.
- xvi. Set EVALUATE_SUPPORT_LEVEL=2 from EVALUATE_SUPPORT_LEVEL=0 and save.
- xvii. Remove the following tag:
<UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs> in the instanceconfig.xml under the tag <Catalog>, present in <Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent and restart all opmn services.
- xviii. Restart all opmn services.
- xix. Disable the cache (cache can be enabled once the setup is moved to the production mode and on the basis of bank's requirements).
- xx. To disable the cache, click "Capacity Management" tab in Oracle Enterprise Manager.
- xxi. Select "Performance" tab within it.
- xxii. Click Lock and Edit Configuration button.
- xxiii. Clear the option "Cache enabled" and then click Activate Changes.
- xxiv. Restart the servers to activate changes. Refer to the following image:



- b. To open the RPD choose Start > All Programs > Oracle Business Intelligence > BI Administration.



- c. Enter the Repository Password as “Administrator1”.
- d. Enter User as “weblogic” and the password provided at the time of installing OBI 11g.
- e. Double click “ConnectionPool1” in the physical layer of the RPD as shown in the following image.



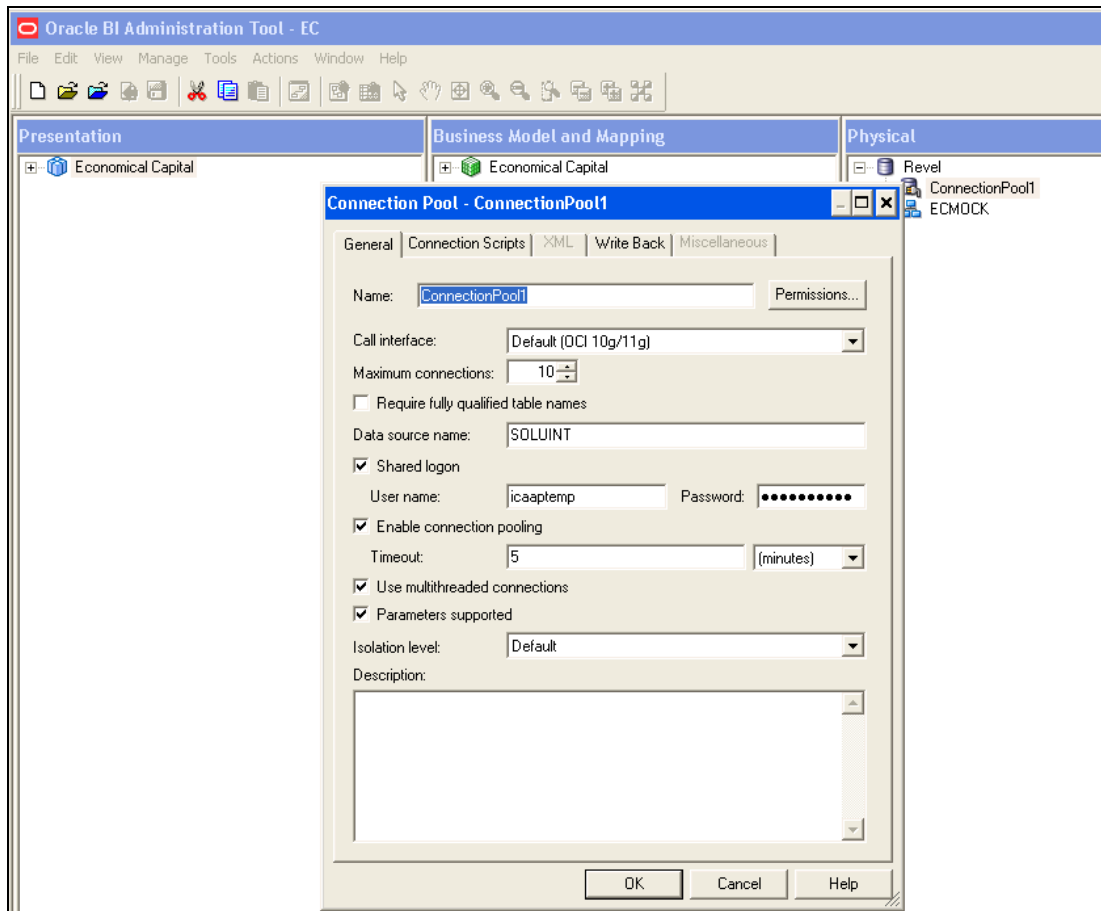
Note:

When the Oracle BI Server is running on Linux or UNIX and you need to update database object settings (such as the database type) or connection pool settings, you can copy the repository file to a Windows computer, make the changes using the Administration Tool on Windows, and then copy the repository file back to the Linux or UNIX computer.

- f. Modify the Data source name, User name and password to the Oracle TNS Name, database schema name and password respectively, as shown in the following image.

Note:

If Oracle TNS Name is entered in **Data Source Name**, then TNS details must be also present under file - *<Installation Path>\Oracle_BI1\network\admin\tnsnames.ora*. Services must be restarted after addition of TNS details in the above mentioned path.



- g. Close the RPD after saving it.
- h. Create a folder named “Credit Risk” (if not created) in the following location “*<OBIEE Installation Path>middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog*” (**Only in case of first time installation**).
- i. Start the following BI services (if not started).

4.3.2 Dashboard/Answer Reports

From any client system that is, windows system:

- j. Start the BI services (if not started).
- k. Start **OBIEE Catalog Manager**.

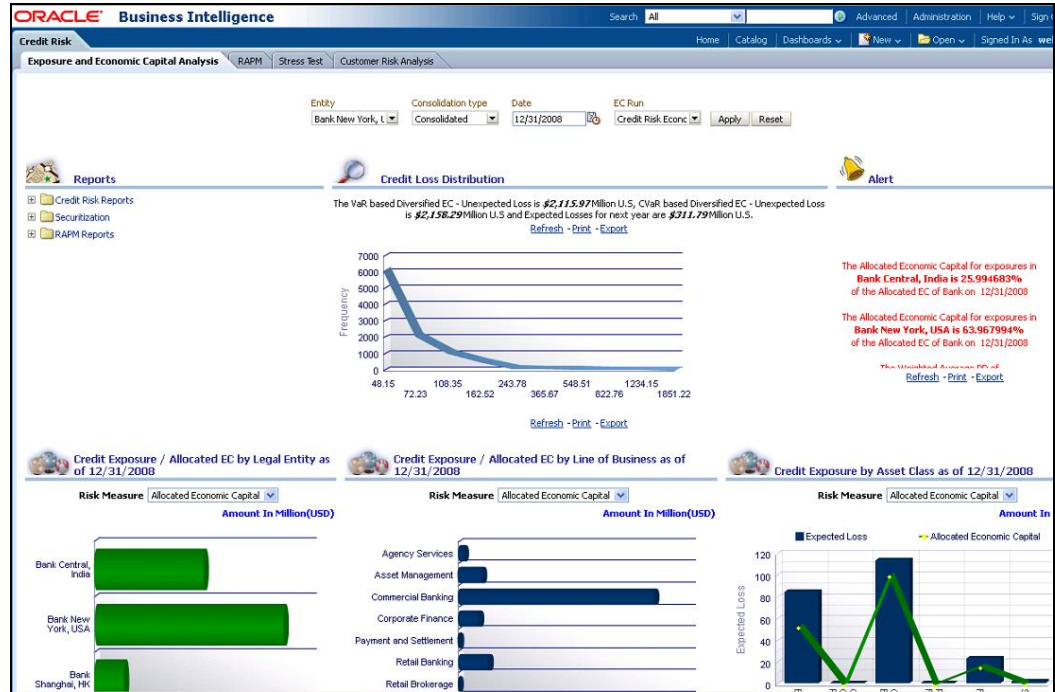
- l. Choose **Start → Programs → Oracle Business Intelligence → Catalog Manager**.
- m. Select **“Open Catalog”** from File menu.
- n. Select the option **“Online”** for Type.
- o. Type the link for presentation services that is, Oracle Interactive Dashboard link. For example (<http://URL:9704/analytics/saw.dll>).
- p. Enter the Administrator User ID and Password, and then click **OK**.
- q. Click **“shared folder”** on the left hand pane.
- r. Select **“Un-archive option”** from File Menu.
- s. Select the archive file **“OFS Economic Capital Advanced – Dashboards”** from the path where it is copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- t. Create a folder name as **“Answers”** (if not created) within **“shared”** folder.
- u. Navigate to **“Answers”** folder.
- v. Select the **“Un-archive”** option from File menu.
- w. Select the archive files **“OFS Economic Capital Advanced - Answers”** from the path where it is copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
- x. Re-Start (stop and start) the BI services.

4.3.3 Installation of Images (Only for New Installation)

- a. Uncompress the file **“OFS Economic Capital Advanced - Images.zip”** and copy all the images to the folder
<OBIEEInstallationPath>\Oracle_BI1\bifoundation\web\app\res\s_blafp\images
- b. Uncompress the file **“OFS Economic Capital Advanced - Images.zip”** and copy all the images to the folder
<OBIEEInstallationPath>
user_projects\domains\bifoundation_domain\servers\bi_server1
tmp\WL_user\analytics_11.1.1\7dezjl\war\res\s_blafp\images
 Or
<OBIEEInstallationPath>
user_projects\domains\bifoundation_domain\servers\AdminServer
tmp\WL_user\analytics_11.1.1\silp1v\war\res\s_blafp\images
- c. Re-Start (stop and start) the BI services.

4.3.4 Post Configuration Verification Steps

- a. Log on to Analytics and verify if the screen looks like the following image:



- b. Click each of the dashboard links, and verify if all the links are visible.
- c. Open the RPD, and verify if the RPD can be accessed online with the Administrator user.

5 OFS Operational Risk Economic Capital Analytics Configuration

5.1 Assumptions

The assumptions for OFS Economic Capital Advanced Analytics Configuration are:

- Oracle Financial Services (OFS) Operational Risk Economic Capital product is installed.
- OBIEE 11.1.1.7.150120 (64-bit) Server for the respective operating system is installed.
- Administrator knows how to start/shutdown the OBIEE servers namely;
 - i. Weblogic Server
 - ii. Oracle BI Server
 - iii. Oracle BI Presentation Server
 - iv. Oracle BI Java Host
- Administrator knows the OBIEE installation path

5.2 Prerequisites

The prerequisites are as follows:

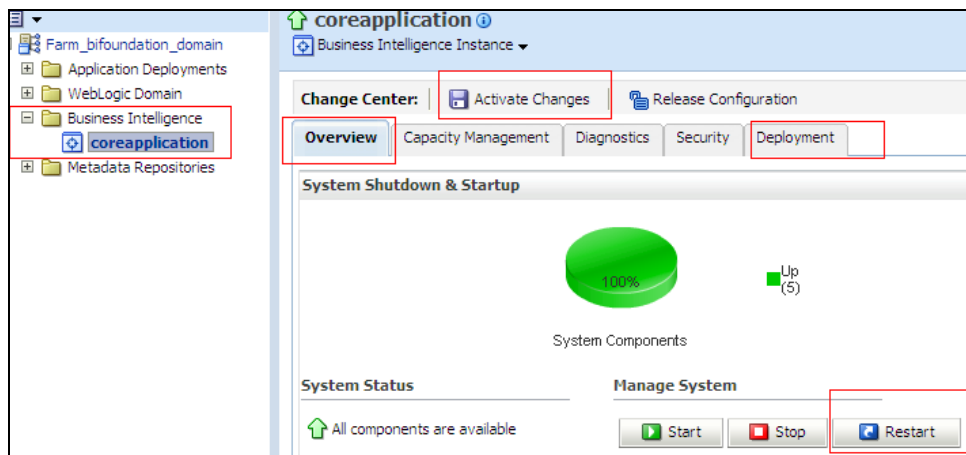
- a. Backup the following OBIEE folders (*for existing installation, not required for new installation*) :
 - *<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIServerComponent\coreapplication_obis1\repository*
 - *<Installation Path>\middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog\<new folder created as part of [Server Configuration Steps](#)>*
- b. Keep OBIEE server details, analytics URL, em URL ready.
- c. Copy following files/folders from the release kit to the local machine:
 - \$FIC_HOME/CAP/catalog/OREC/; this folder has the **OFS Operational Risk Economic Capital Analytics.catalog** file for dashboard (reports).
 - \$FIC_HOME/CAP/repository/; this has the **OFS Operational Risk Economic Capital Analytics - Repository.rpd** file. Unzip this file on the local machine.

5.3 Configuration Steps

5.3.1 Server Configuration Steps

Perform the following Server Configuration steps for each release (follow these instructions for the server setup):

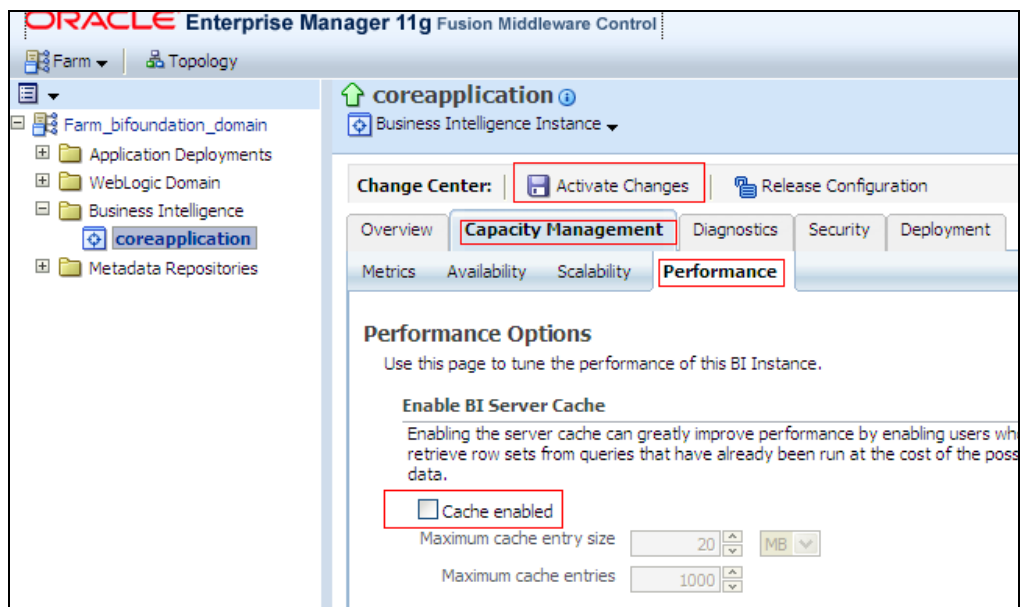
- a. Add the **tnsnames.ora** file in the following folder “<Installation Path>middleware\Oracle_BI1\network\admin”. The **tnsnames.ora** file should contain the data-source connection details used in the connection pool of the RPD.
- b. Log on to Oracle Enterprise Manager.
 - i. Go to **Business Intelligence** menu located on the left hand side of the screen. Select **coreapplication** within it.
 - ii. Go to **Deployment** located on the last tab.
 - iii. Click **Lock and Edit Configuration**.
 - iv. Go to the section **Upload BI Repository**.
 - v. Browse and select the repository.
 - vi. Enter the repository password and confirm the same. The repository password is “Administrator1”.
 - vii. Go to **BI Presentation Catalog** section.
 - viii. Edit the catalog path and remove SampleAppLite (Only in case of first time installation) from the end of the catalog path section and enter OREC as the name of the new catalog folder. Make sure that the folder path is <OBIEE Installation Path>middleware\instances\instance1\bifoundation\OracleBIPresentationServices Component\coreapplication_obips1\catalog\OREC
 - ix. Click **Apply**.
 - x. Click **Activate Changes**.
 - xi. Click **Overview** tab.
 - xii. Click **Restart**.



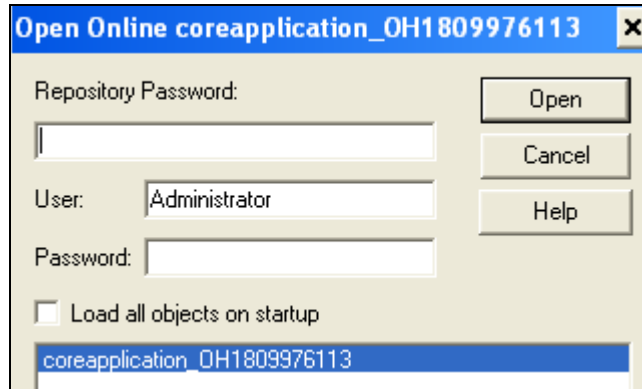
- xiii. Confirm to restart all opmn services.

NOTE: Note: Step (xiv) to (xxi) must be followed only during the first time of configuration.

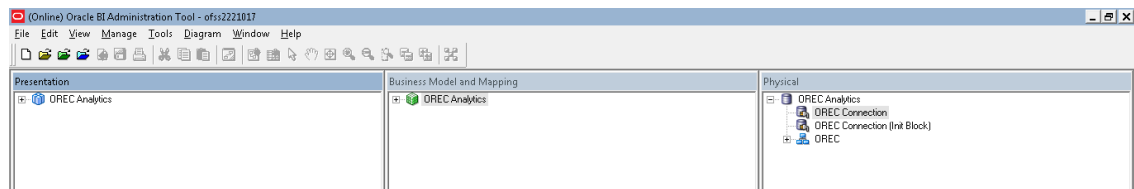
- xiv. Edit the **NQSConfig.INI** file, found at <Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1 to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = NO to YES.
- xv. Add the tag <UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs> in the **instanceconfig.xml** under the tag <Catalog>, found at <Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent and
- xvi. Restart all opmn services.
- xvii. Check if all the servers are up and running (except Presentation Service).
- xviii. Edit the **NQSConfig.INI** file, found at <Installation Path>\instances\instance1\config\OracleBIServerComponent\coreapplication_obis1 to reset the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES to NO. Set EVALUATE_SUPPORT_LEVEL=2 from EVALUATE_SUPPORT_LEVEL=0 and save.
- xix. Remove the tag <UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs> in the **instanceconfig.xml** under the tag <Catalog>, found at <Installation Path>\instances\instance1\config\OracleBIPresentationServicesComponent.
- xx. Restart all opmn services.
- xxi. Disable the cache (cache can be enabled once the setup is moved to the production mode and on the basis of bank's requirements). To disable the cache, click "Capacity Management" tab in the Oracle Enterprise Manager. Select "Performance" tab within it. Click 'Lock and Edit Configuration' button. Un-check the option "Cache enabled". Click Activate Changes. Restart the servers to activate changes. Refer to the following figure.



- c. Open the RPD (via **Start → All Programs → Oracle Business Intelligence → BI Administration**).



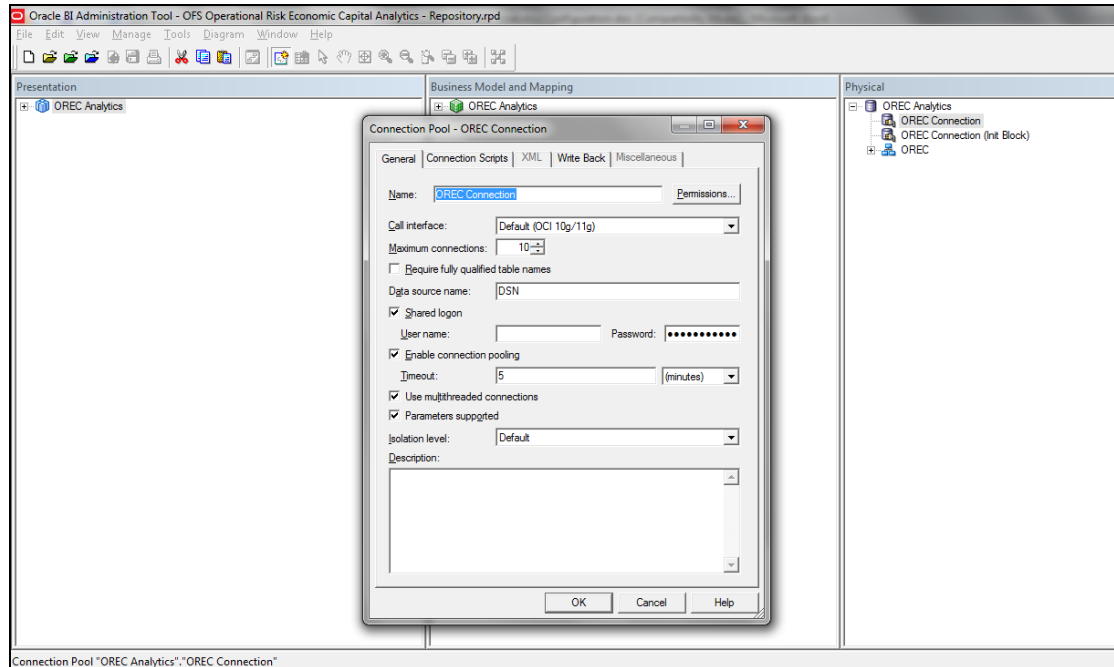
- d. Provide the Username and Password which have access to open RPD online and the Repository Password as “Administrator1”.
- e. Double-click “**OREC Connection**” Connection Pool in the physical layer of the RPD as shown in the following figure:



NOTE: When the Oracle BI Server is running on Linux or UNIX and you need to update database object settings (such as the database type) or connection pool settings, you can copy the repository file to a Windows computer, make the changes using the Administration Tool on Windows, and then copy the repository file back to the Linux or UNIX computer.

- f. Change data source name, user name and password to the Oracle TNS Name, database schema name and password respectively, as shown in the following figure.

NOTE: If Oracle TNS Name is entered in **Data Source Name**, then TNS details must be also present under file:
`<Installation Path>\Oracle_BI1\network\admin\tnsnames.ora`. Services must be restarted after addition of TNS details in the above mentioned path.



- g. Similarly, change the details for “**OREC Connection (Init Block)**”
- h. Save the **RPD**.
- i. Close the **RPD**.
- j. Restart the **opmn** services.

5.3.2 Dashboard/Answer Reports

Configure the **OREC Dashboard** via **Catalog Deployment** with these steps:

- a. Login to **Analytics URL**.
- b. Click **Catalog** link.
- c. Click **Shared Folder** in the left hand pane.
- d. Select **Un-archive** to un-archive **OFS Operational Risk Economic Capital Analytics.catalog** file, copied onto the local machine as part of introduction pre-requisite step.
- e. Click **OK**.

6 Data Privacy Features Implementation by OFSAA

Data privacy refers to the protection of data against unauthorized access and data theft. OFSAA ensures Data privacy with the following features:

- Data Redaction
- Right to be Forgotten
- Data Privacy for OBIEE

6.1 Data Redaction

OFS CAP is enhanced to enable masking of sensitive data and Personal Identification Information (PII) to adhere to Regulations and Privacy Policies. Oracle Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed to a pattern that does not contain any identifiable information.

6.1.1 Prerequisites

- Ensure the required Oracle Database Server versions are installed.
Oracle 12c (from 11.2.0.4) – as part of oracle advanced security, which should be separately licensed.
- **Instance level flag to set redaction feature ON/OFF:**
Login as SYSDBA and check if the instance level data redaction feature is enabled using the below query:

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Data Redaction';
```

The result returned must be "Y".

- **Schema creator changes for DATA_REDACT and TDE feature.**

The following section must to be enabled in "OFS_CAP_ADQ_SCHEMA_IN.xml" during schema creation. Refer IG input

```
<ADV_SEC_OPTIONS>
```

```
<OPTION NAME="TDE" VALUE="FALSE"/>
```

```
<OPTION NAME="DATA_REDACT" VALUE="TRUE" />
```

```
</ADV_SEC_OPTIONS>
```

```
<TABLESPACES>
```

```
<TABLESPACE NAME="OFSAA_CONF_TBSP" VALUE="OFSAA_CONF" DATAFILE=""  
SIZE="128M" AUTOEXTEND="ON" ENCRYPT="OFF" />
```

```
<TABLESPACE NAME="OFSAA_DATA_TBSP" VALUE="OFSAA_DATA" DATAFILE=""  
SIZE="512M" AUTOEXTEND="ON" ENCRYPT="OFF" />
```

```
</TABLESPACES>';
```

- **Configuration Schema changes:**

Enable Data Redaction at application level by executing below query in config schema:

```
UPDATE configuration SET PARAMVALUE = 'Y' WHERE PARAMNAME =  
'IS_DATA_REDACTION_ENABLED';
```

The flag is disabled by default (value – N).

6.1.2 Executing Data Redaction Utility

Following are the steps if you want to execute Data Redaction Utility:

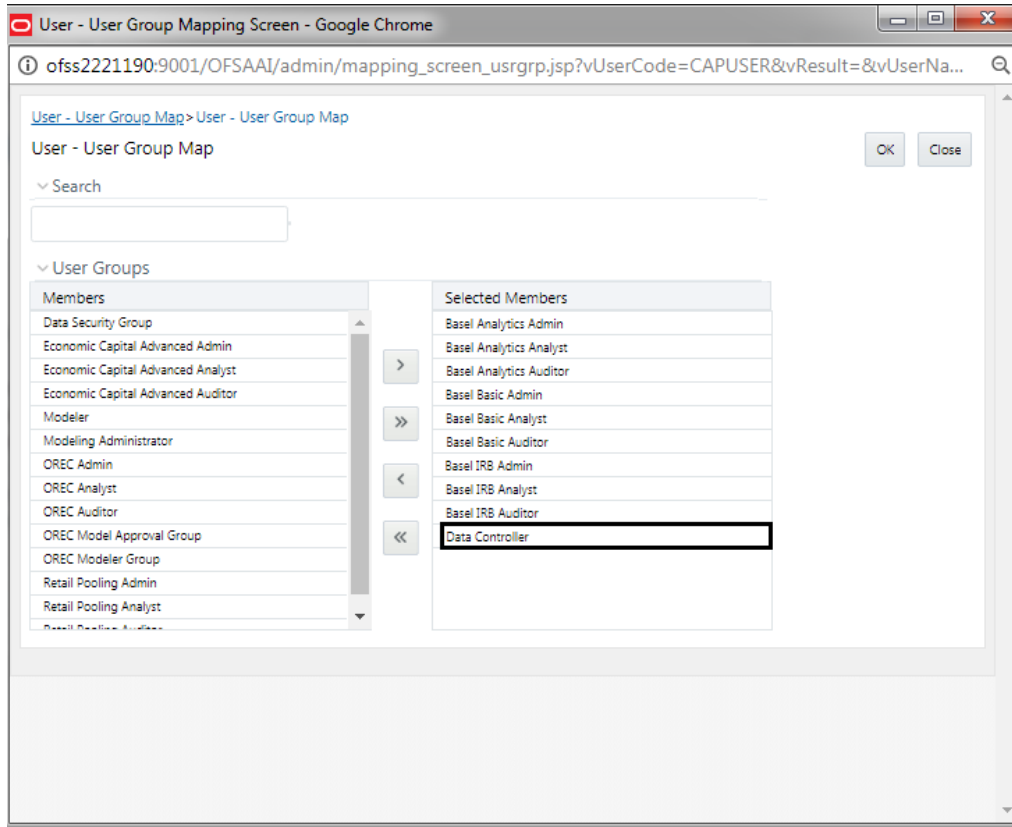
1. Login as SYSDBA and execute the following SQL statement.

```
grant execute on DBMS_REDACT to &atomicUser  
  
/  
  
Create role OFS_SEC_DATA  
  
/  
  
grant OFS_SEC_DATA to &atomicUser  
  
/  
  
create role OFS_NOSEC_DATA  
  
/  
  
grant EXEMPT REDACTION POLICY to OFS_NOSEC_DATA  
  
/  
  
grant OFS_NOSEC_DATA to &atomicUser  
  
/  
  
alter user &atomicUser default role none  
  
/
```

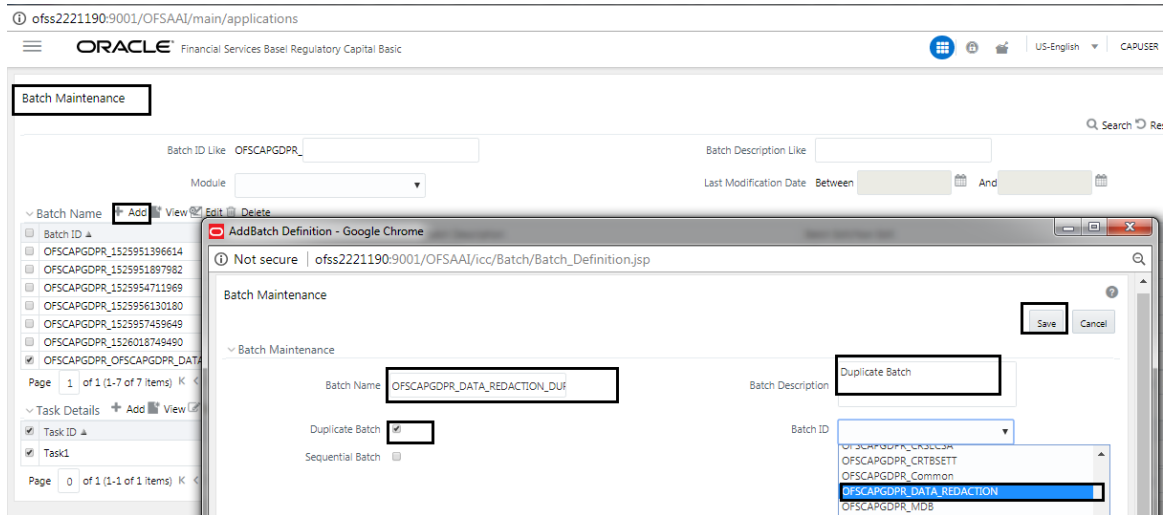
2. Login into Configuration schema and execute the following SQL statement.

```
grant select on cssms_usr_group_map_view to &atomicUser  
  
/  
  
grant execute on checkEnvForDataRedaction to &atomicUser  
  
/
```

3. Login into OFS CAP with SYSADMN user.
 4. Navigate to the **User – User Group Mapping** screen and assign Data Controller user group to the batch owner.
-



5. Login into OFS CAP with the desired user name.
6. Navigate to the **Batch Maintenance** screen and create duplicate batch as the original batch is not editable and batch parameter must be changed.



7. Edit the Task and change the user (user assigned to Data Controller group).

Task Definition Save Close

Task ID: Task1 Description: Data Redaction

Components: RUN EXECUTABLE

Dynamic Parameters List

Property	Value
Datastore Type	EDW
Datastore Name	OFSCAPGDPR
Primary IP For Runtime Processes	ofss2221190
Executable	dataredaction.sh,false,CAPUSER
Wait	N
Batch Parameter	Y
Optional Parameters	NULL

Audit Panel

Created By: CAPUSER Creation Date: 11 may 2018 11:55:57
 Last modified by: CAPUSER Last Modification Date: 11 may 2018 11:55:57

8. Execute the **Data Redaction** (duplicate) batch for the desired FIC_MIS_DATE. For example, in the below image it is 04-Jan-2014.

Batch Details Schedule Batch

Batch ID	Batch Description
<input type="checkbox"/> OFSCAPGDPR_1525951396614	FullFRTB
<input type="checkbox"/> OFSCAPGDPR_1525951897982	FRTB_Full
<input type="checkbox"/> OFSCAPGDPR_1525954711969	AutoRun_1519753300689_Descr
<input type="checkbox"/> OFSCAPGDPR_1525956130180	KKKKKKKKKKKK
<input type="checkbox"/> OFSCAPGDPR_1525957459649	KKKKK123
<input type="checkbox"/> OFSCAPGDPR_BASEL_COMMON	COMMON
<input type="checkbox"/> OFSCAPGDPR_BASEL_DAILY	DAILY
<input checked="" type="checkbox"/> OFSCAPGDPR_DATA_REDACTION	Batch for Data Redaction
<input type="checkbox"/> OFSCAPGDPR_RightToForget	Batch for Right To Forget
<input type="checkbox"/> OFSCAPGDPR_SCD	SCD

Page 1 of 1 (1-10 of 10 items) K < > X

Task Details Exclude/Include Hold/Release

Task ID	Task Description	Metadata Value	Component ID	Pr
Task1	Data Redaction	dataredaction.sh,false,CAPUSER	RUN EXECUTABLE	

Page 1 of 1 (1-1 of 1 items) K < > X

Information Date

Date: 01/04/2014 📅

Execute Batch

6.2 Right to be Forgotten

Right to be Forgotten is the task of removing PII (Personally Identifiable Information) of a Data Subject for the given Party. The financial institution can delete PII for those Data Subjects who have requested this Right to be Forgotten functionality.

The Data Subjects may have made significant financial transactions, and/or financial information may be required for regulatory or compliance reporting. Deleting the complete record that consists of PII may lead to issues in data reconciliation. In OFSAA, the PII data will be replaced with randomized values and therefore, the complete Data Subject record is retained. As a result, financial information is retained; however, the associated Party PII is removed permanently.

6.2.1 Prerequisites

Use the FSI_PARTY_RIGHT_TO_FORGET table to collect the input list of Party IDs for which PII must be removed from the system. The financial institution must source this Party ID list into the FSI_PARTY_RIGHT_TO_FORGET table, and then invoke the batch (<<INFODOM>>_RightToForget) or schedule it.

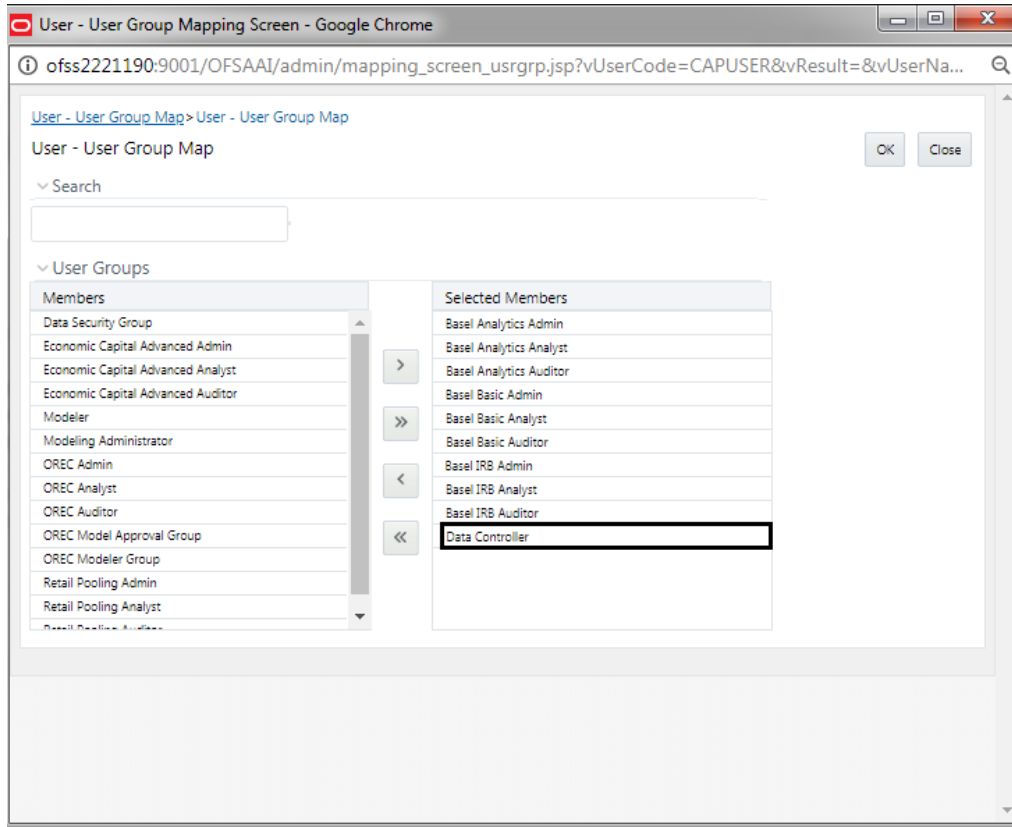
NOTE: For sample query, see Sample Query for the FSI_PARTY_RIGHT_TO_FORGET table.

Refer OFS Data Foundation Data Protection Implementation Guide (Release 8.0.6.0.0) in [OHC](#) for more details.

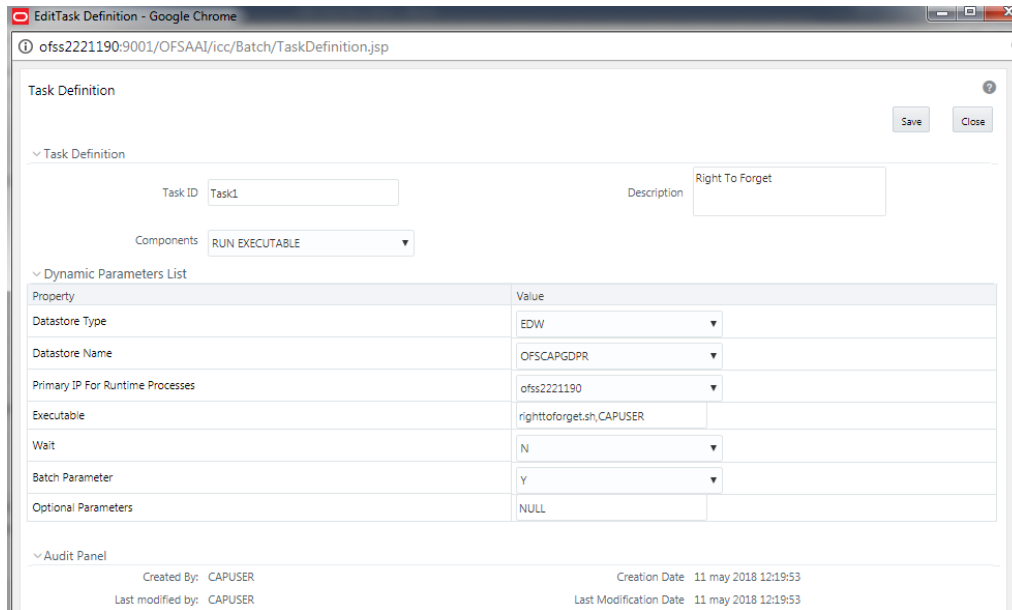
6.2.2 Executing Right to be Forgotten Utility

Following are the steps if you want to execute Right to be Forgotten Utility:

1. Login into OFS CAP as SYSADMN.
2. Navigate to the **User – User Group Mapping** screen and assign Data Controller user group to the batch owner.



3. Login into OFS CAP with the desired user name.
4. Navigate to **Batch Maintenance** screen and create duplicate batch as the original batch is not editable and batch parameter must be changed.



5. Execute the **Right To Forget** (duplicate) batch for the desired FIC_MIS_DATE. For example, in the below image it is 04-Jan-2014

<input checked="" type="checkbox"/>	OFSCAPGDPR_OFSCAPGDPR_RightToForget_DUP	Right To Forget Duplicate Batch
<input type="checkbox"/>	OFSCAPGDPR_RightToForget	Batch for Right To Forget
<input type="checkbox"/>	OFSCAPGDPR_SCD	SCD


Page 1 of 1 (1-13 of 13 items) K < > X

Task Details Exclude/Include Hold/Release

ask ID	Task Description	Metadata Value	Component ID	Precedence
ask1	Right To Forget	righttoforget.sh,CAPUSER	RUN EXECUTABLE	

Page 1 of 1 (1-1 of 1 items) K < > X

Information Date

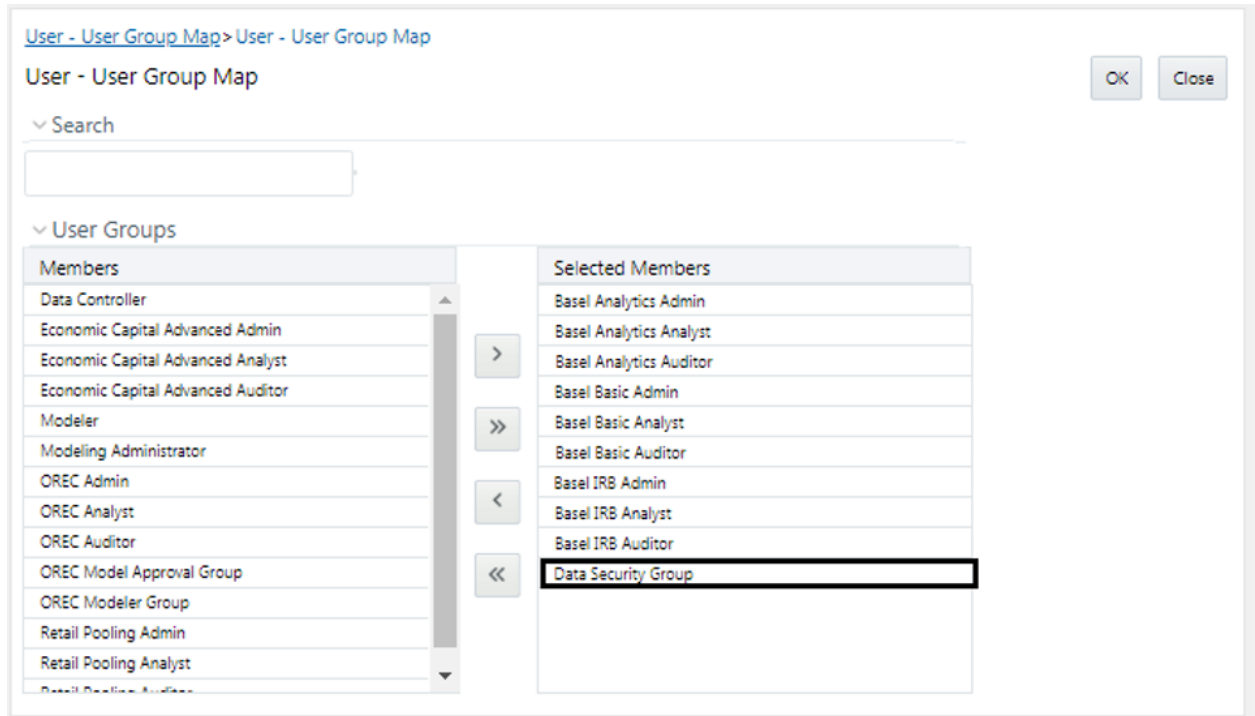
Date 01/04/2014 

Execute Batch

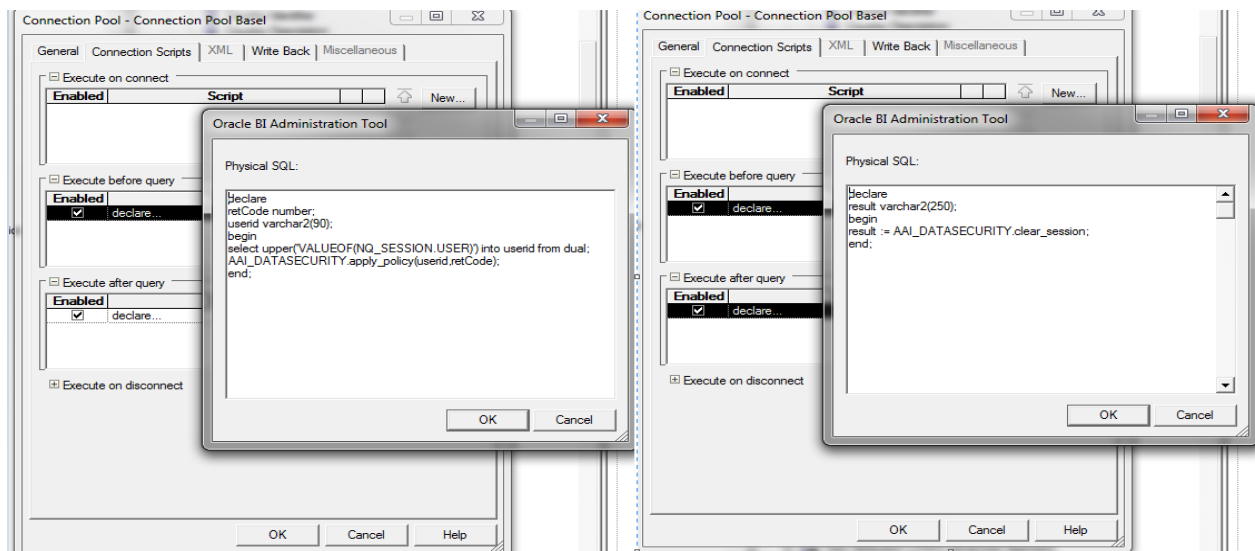
6.3 Data Privacy for OBIEE

6.3.1 Prerequisites

1. Login to OFS CAP application as SYSADMN.
2. Navigate to **User – User Group Map** screen. Map the Data Security Group to the user.



3. Make the following changes to the RPD.



- a. Edit Connection pool and update the 'Execute After Query' as:

```
declare
```

```
result varchar2(250);  
begin  
result := AAI_DATASECURITY.clear_session;  
end;
```

- b. Edit Connection pool and update the 'Execute Before Query' as:

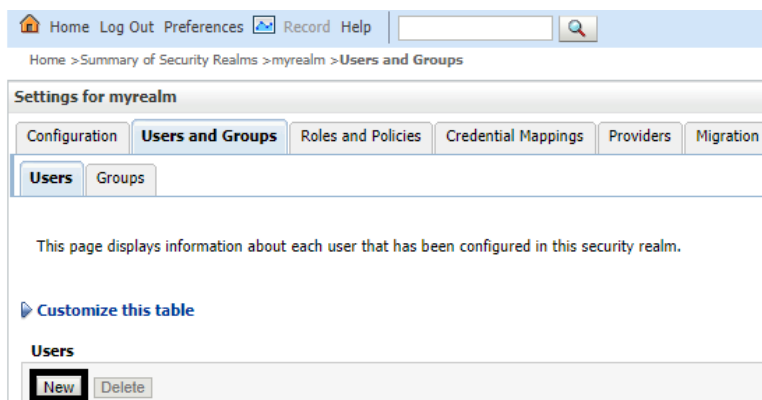
```
declare  
  
retCode number;  
  
userid varchar2(90);  
  
begin  
  
select upper('VALUEOF(NQ_SESSION.USER)') into userid from  
dual;  
  
AAI_DATASECURITY.apply_policy(userid,retCode);  
  
end;
```

6.3.2 Executing OBIEE Utility

Following are the steps if you want to execute OBIEE Utility.

1. Login to OBIEE console for adding user and groups.
2. Navigate to Home > Summary of Servers > Summary of Security Realms > myrealm > Users and Groups.
3. Create a new user with the same name as the OFS CAP user (with Data Security Group mapped) as shown in the below images.

USER



Create a New User

User Properties

The following properties will be used to identify your new User.
* Indicates required fields

What would you like to name your new User?

* **Name:**

How would you like to describe the new User?

Description:

Please choose a provider for the user.

Provider:

The password is associated with the login name for the new User.

* **Password:**

* **Confirm Password:**

> Audit Panel

Created By: CAPUSER
Last modified by: CAPUSER

Creation Di
Last Modification Di

4. Create a new group with the name UGDSREPPII as shown in the below images.

GROUP

Home Log Out Preferences Record Help

Home > Summary of Security Realms > myrealm > Users and Groups > testuser > Users and Groups

Settings for myrealm

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

Users **Groups**

This page displays information about each group that has been configured in this security realm.

[Customize this table](#)

Groups

<input type="checkbox"/>	Name ↕	Description
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.

Create a New Group

Group Properties

The following properties will be used to identify your new Group.
* Indicates required fields

What would you like to name your new Group?

* Name:

How would you like to describe the new Group?

Description:

Please choose a provider for the group.

Provider:

5. Assign user to this group (User who can see the redacted data).

Settings for OBIEE_USER

Use this page to configure group membership for this user.

Parent Groups:

Available:		Chosen:
<input type="checkbox"/> AdminChannelUsers		<input type="checkbox"/> UGDSREPII
<input type="checkbox"/> Administrators	>	
<input type="checkbox"/> AppTesters	<>	
<input type="checkbox"/> BIAdministrators	<	
<input type="checkbox"/> BIAuthors		
<input type="checkbox"/> BICongsumers	<>	
<input type="checkbox"/> BSLBIANALYST		
<input type="checkbox"/> CrossDomainConnectors		

6. Login as the user created above and any other user to verify Data Redaction / Right to forget.



Oracle Financial Services Capital Adequacy Pack - Release 8.0.6.0.0 Admin Guide

May 2018
Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
<http://www.oracle.com/us/industries/financial-services/index.html>

Copyright © 2018 Oracle Financial Services Software Limited. All rights reserved.

No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.

Due care has been taken to make this Admin Guide and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this Admin Guide and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.

All company and product names are trademarks of the respective companies with which they are associated.
