# Admin Guide
# Oracle Financial Services Basel Regulatory Capital Analytics
# Release 6.1.0.0.0

January 2014

## Document Control

| Version Number | Revision Date | Changes Done |
|---|---|---|
| Version 6.1 | Created on August 2013 | Captured the administration activities for 6.1.0.0.0 Release enhancements. |
| 6.1 (6.0-6.1 Upgrade) | Revised on January 2014 | Updated the 6.0-6.1 upgrade related information and updated the suggested reviewed changes. |
| Created and Edited by: Sindhu/Swathi | Reviewed By : Aju/Ranjit | Approved by : Kumaran |

### Executive Summary

The document includes the necessary instructions for module specific configurations. We recommend you to download the latest copy of this document from OTN library which includes all the recent additions/revisions (if any) done till date.

# TABLE OF CONTENTS


1 ORACLE FINANCIAL SERVICES BASEL REGULATORY CAPITAL ANALYTICS 6.1.0.0.0 CONFIGURATION ..... 1

1.1 Introduction ..... 1

1.1.1 Assumptions ..... 1

1.1.2 Prerequisites ..... 1

1.2 Configuration Steps ..... 2

1.2.1 Script Execution ..... 2

1.2.2 Server Configuration steps: ..... 2

1.2.3 Application Roles ..... 6

1.2.4 Dashboard/Answer Reports (from any client machine i.e. windows machine): ..... 6

1.2.5 Installation of Images (Only for New Installation): ..... 9

1.2.6 BI Publisher Reports (Only for New Installation): ..... 9

1.3 Post configuration verification steps ..... 10

1.4 Configuring OBIEE link in OFSAAI Framework ..... 11

2 ORACLE FINANCIAL SERVICES ELECTRONIC SUBMISSION ADMINISTRATION ACTIVITIES ..... 13

2.1 User Administrator ..... 13

2.1.1 User Maintenance ..... 13

2.1.2 UserGroup Maintenance ..... 17

2.1.3 User UserGroup Map ..... 19

2.1.4 Profile Maintenance ..... 20

2.1.5 User Authorization ..... 23

2.1.6 User Group Authorization ..... 24

2.1.7 UserGroup Domain Map ..... 25

2.1.8 UserGroup Role Map ..... 26

2.2 System Administrator ..... 29

2.2.1 Assumptions: ..... 29

2.2.2 Pre-Requisites: ..... 30

2.2.3 Installing and Configuring SMTP on Web Application Server ..... 30

2.2.4 Creating a New Access Control List ..... 31

2.2.5 Access of Web Application Server to SMTP server ..... 33

2.2.6 Data Preparation for Mail Utility ..... 33

2.2.7 SETUP DATA: ..... 49

2.2.8 MASKING DATA PREPARATION ..... 52

# 1 Oracle Financial Services Basel Regulatory Capital Analytics 6.1.0.0.0 Configuration

## 1.1 Introduction

### 1.1.1 Assumptions

- If Oracle Financial Services (OFS) Basel Regulatory Capital product is installed, then the table scripts need not be executed as described in Section 1.2.1 of this document.
- If OFS Basel Regulatory Capital Analytics is deployed without the OFS Basel Regulatory Capital product, then the table scripts that are provided with the Analytics release should be executed in a new and blank database schema (refer Section 1.2.1 and Section 1.2.2 for more details).
- The database schema will have proper privileges namely: **`CONNECT, RESOURCE AND CREATE MATERIALIZED VIEW,`** to execute the above mentioned scripts.
- OBIEE 11.1.1.6.10 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.

### 1.1.2 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 Installation 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:

**With Oracle Financial Services Basel Regulatory Capital**

- $FIC_HOME/BASELBI/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/BASELBI/*repository/*OFS Basel Regulatory Capital Analytics 6.1 - Repository.zip; this has the Basel.rpd file. Unzip this file on the local machine.

- $FIC_HOME/BASELBI/Images/OFS Basel Regulatory Capital Analytics 6.1 - Images.zip; this has image files which are used in the reports (for new installation). Unzip this file in the local machine.
- $FIC_HOME/BASELBI/dashboardconfiguration/CreateAppRoles.py; this is a script which is used for application role creation (for new installation).

**Note:** During multi-tier installation, $FIC_HOME/BASELBI/ directory will be available in DB Layer.

## 1.2 Configuration Steps

### 1.2.1 Script Execution

Execute the following scripts (from *Customer Deliverables**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

### 1.2.2 Server Configuration steps:

For each release, confirm that the following has been 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.

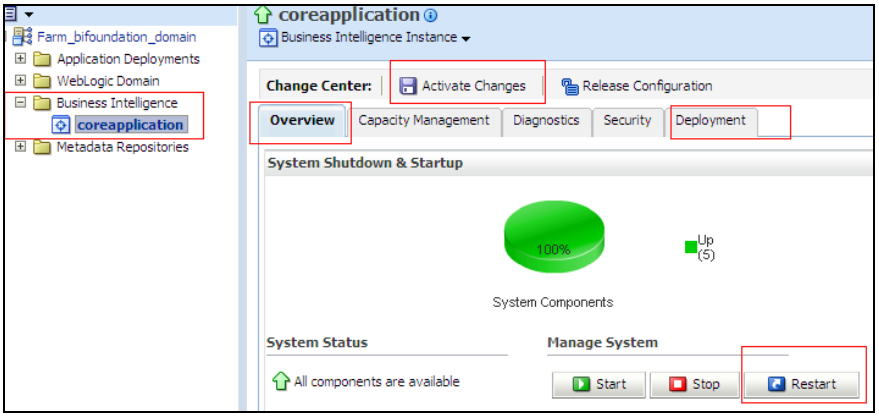
viii. Edit the catalog path and remove SampleAppLite (Only in case of first time installation) from the end of the catalog path section and enter Basel as the name of the new catalog folder. Make sure that the folder path is *<OBIEE Installation Path>middleware\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog*

ix. Click **Apply**.

x. Click **Activate Changes.**

xi. Click **Overview** tab.

xii. Click **Restart**.




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 and update.

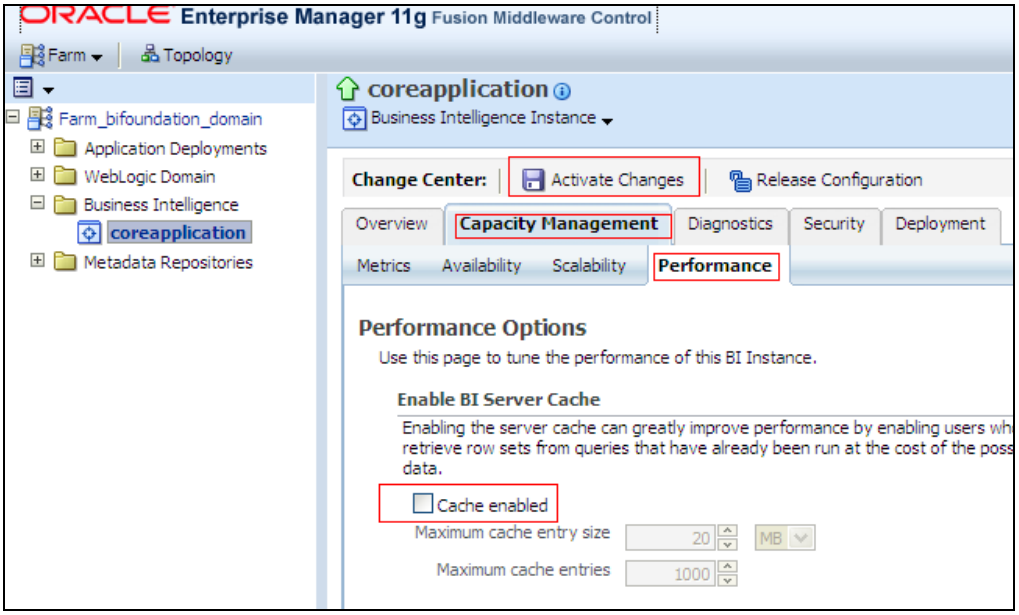
Set EVALUATE_SUPPORT_LEVEL=2 from EVALUATE_SUPPORT_LEVEL=0 and save.

xviii. Remove the tag <UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs> in the ***instanceconfig.xml*** under the tag ***<Catalog>***, found at *<Installation*

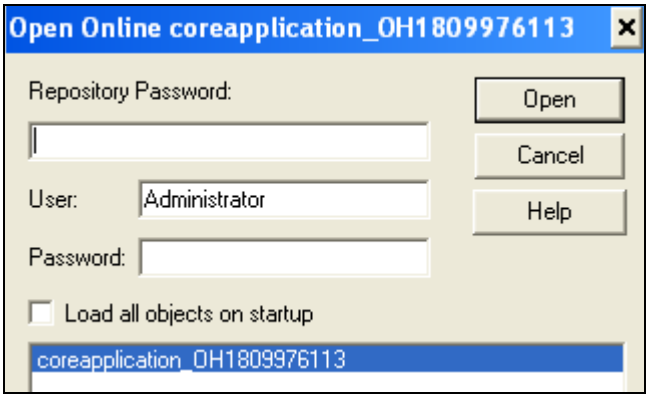
*Path>\instances\instance1\config\OracleBIPresentationServicesComponent* and restart all opmn services.

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 on Activate Changes. Restart the servers to activate changes. Refer to the image below.

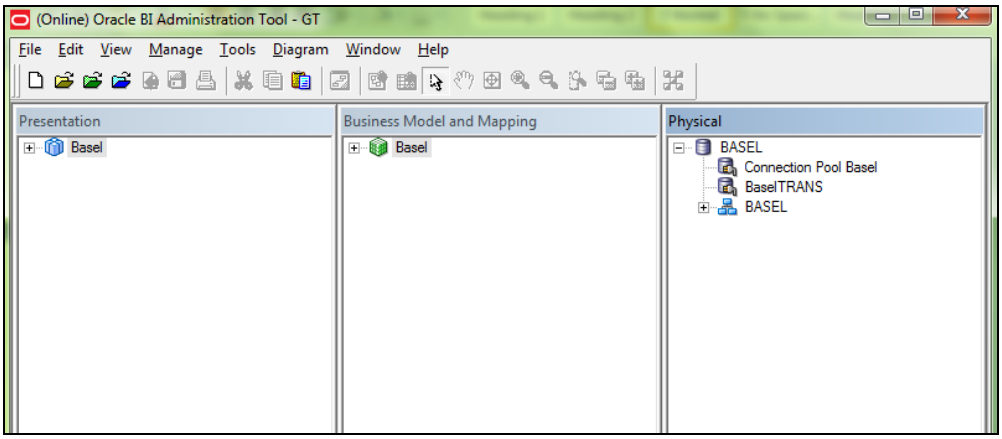



c. Open the RPD by clicking start menu > All Programs > Oracle Business Intelligence > BI Administration



d. Provide the User and password as web logic and the password provided at the time of installing OBI 11g 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:



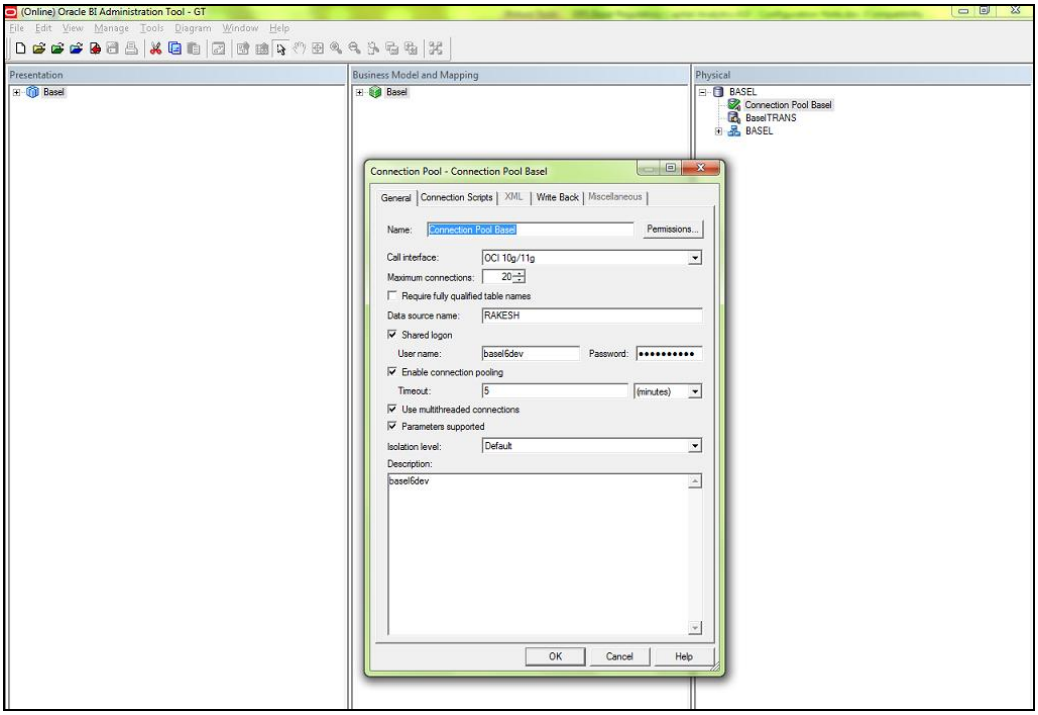

**Note:**

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. Create a folder named **"Basel"** (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**)

j. Restart the opmn services.

### 1.2.3 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*

### 1.2.4 Dashboard/Answer Reports (from any client machine i.e. 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 1.2.6 after un-archiving files for BI Publisher Reports (Only for New Installation).

1. **Configuring Basel**
   i. Click the *"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 6.1 - Basel_Dashboard"* (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
   iii. Create a folder *"Answers"* under *"shared folder".*
   iv. Click on the folder *"Answers"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - Basel_Answers"* (sent as release).
   v. Re-Start (stop and start) the BI services.

2. **Configuring US**
   i. Click on the *"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 6.1 - US_Dashboard"* (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK.**
   iii. Create a folder *"Answers"* under *"shared folder".*
   iv. Click on the folder *"Answers"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - US_Answers"* (sent as release).
   v. Create a folder *"BIP_REPORTS"* under *"shared folder".*
   vi. Click on the folder *"BIP_REPORTS"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - US_BIP"* (sent as release).
   vii. Re-Start (stop and start) the BI services.

3. **Configuring FINMA**
   i. Click the *"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 6.1 - FINMA_Dashboard"* (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
iii. Create a folder *"Answers"* under *"shared folder"* (Do not recreate, if created in Step 2 of section 1.2.3).
iv. Click on the folder *"Answers"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - FINMA_Answers"* (sent as release).
v. Create a folder *"BIP_REPORTS"* under *"shared folder"* (Do not recreate, if created in Step 2 of section 1.2.3).
vi. Click on the folder *"BIP_REPORTS"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - FINMA_BIP"* (sent as release).
vii. Re-Start (stop and start) the BI services.

**4. Configuring Islamic Banking**

i. Click the *"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 6.1 - IFSB_Dashboard"* (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
iii. Create a folder *"Answers"* under *"shared folder"* (Do not recreate, if created in Step 2 of section 1.2.3).
iv. Click on the folder *"Answers"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - IFSB_Answers"* (sent as release).
v. Re-Start (stop and start) the BI services.

**5. Configuring CBRC**

i. Click the *"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 6.1 - CBRC_Dashboard"* (sent as release), copied onto the local machine as part of introduction pre-requisite step, and click **OK**.
iii. Create a folder *"BIP_REPORTS"* under *"shared folder"* (Do not recreate, if created in Step 2 of section 1.2.3).
iv. Click on the folder *"BIP_REPORTS"* and un-archive file *"OFS Basel Regulatory Capital Analytics 6.1 - CBRC_BIP"* (sent as release).
v. Re-Start (stop and start) the BI services.

### 1.2.5 Installation of Images (Only for New Installation):

a. Uncompress the file "*OFS Basel Regulatory Capital Analytics 6.1 - Images.zip*" 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 6.1 - 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\7dezjl\war\res\s_blafp\images.*

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

### 1.2.6 BI Publisher Reports (Only for New Installation):

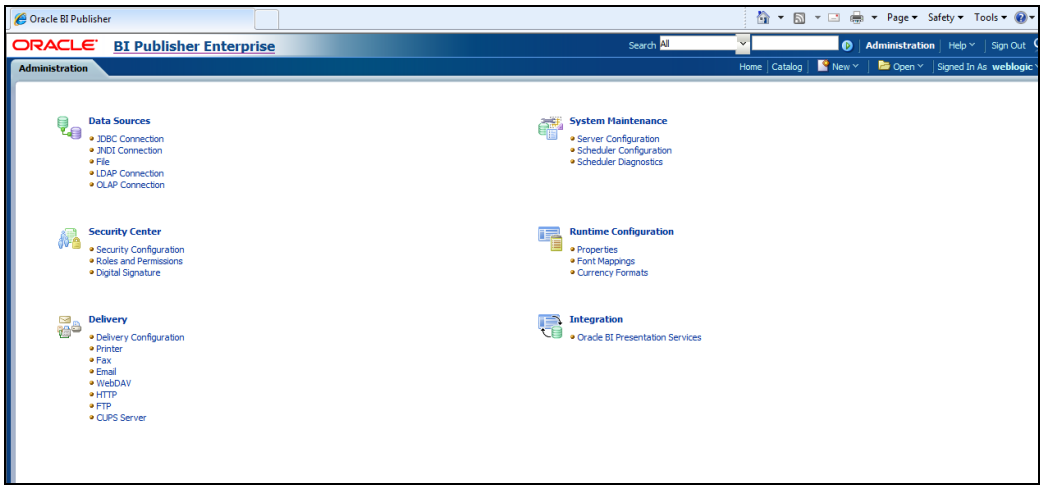
a. Type the link for Oracle BI Publisher link.

For example: *http://URL:<port_number>/xmlpserver*

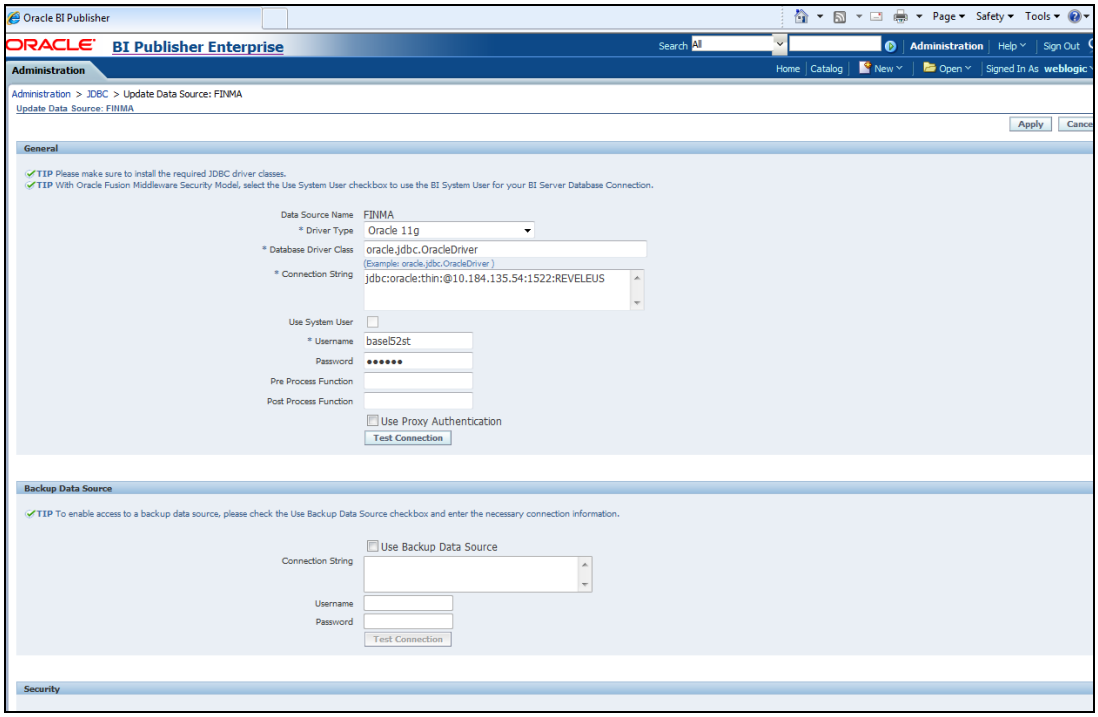
c. Login through Administrator user Id and password.

d. Click **Administration** (available at top right of the page).

e. Click **JDBC Connection**, available under Data Sources.




f. 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.

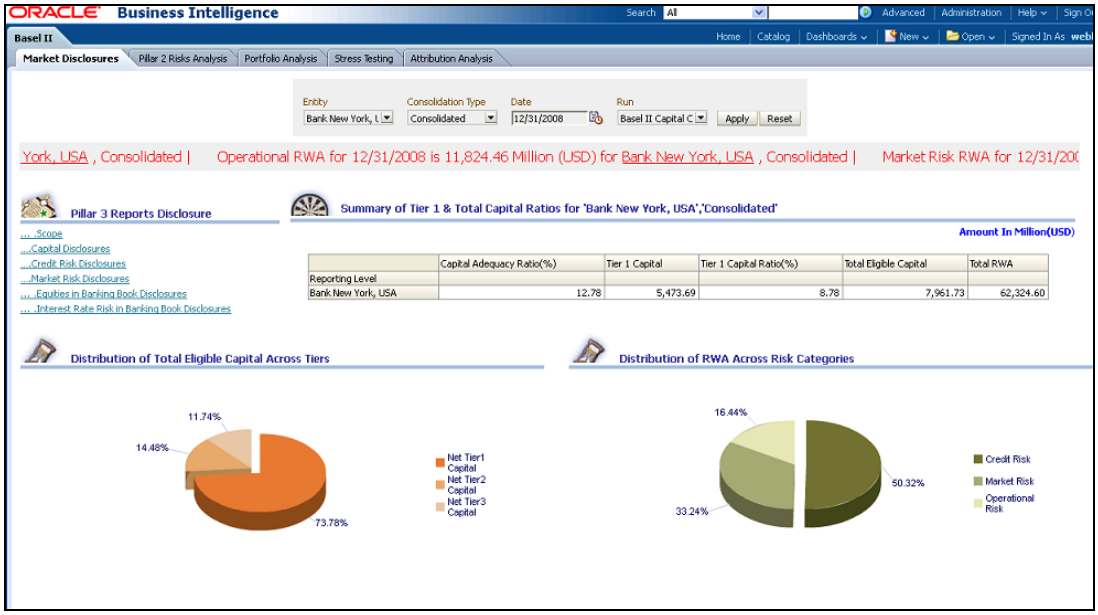
Click **Apply.**

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

g. Similarly add two more data sources with names "***ERM***" and "***CBRC***", as described in the above step e.

## 1.3 Post configuration verification steps

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



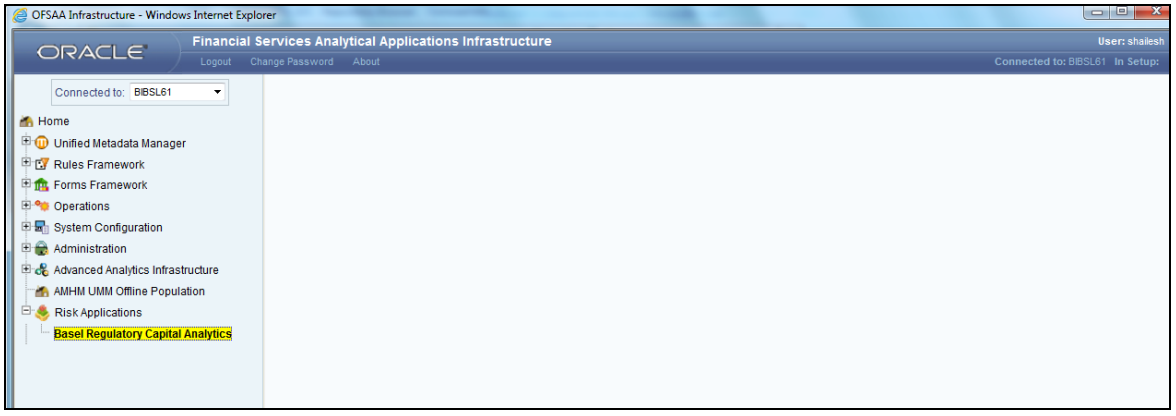

b. Click each of the dashboard links, and check if all the links are visible.

Open the RPD, and check if the RPD can be accessed online with the Administrator user.

## 1.4 Configuring OBIEE link in OFSAAI Framework

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

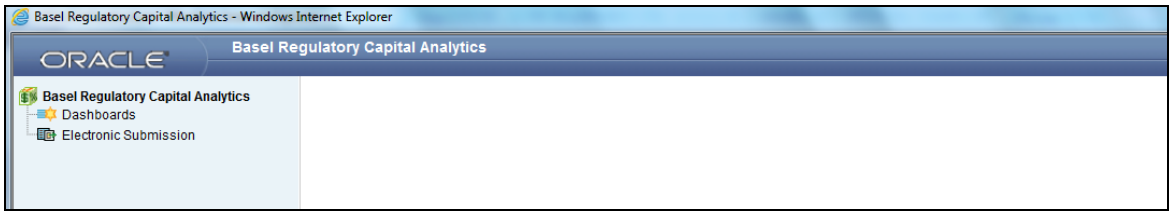
Under **Risk Applications**, click **Basel Regulatory Capital Analytics** option.




The Basel Regulatory Capital 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 https://flexsupp.oracle.com/.Analytics

# 2 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.

## 2.1 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

### 2.1.1 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.

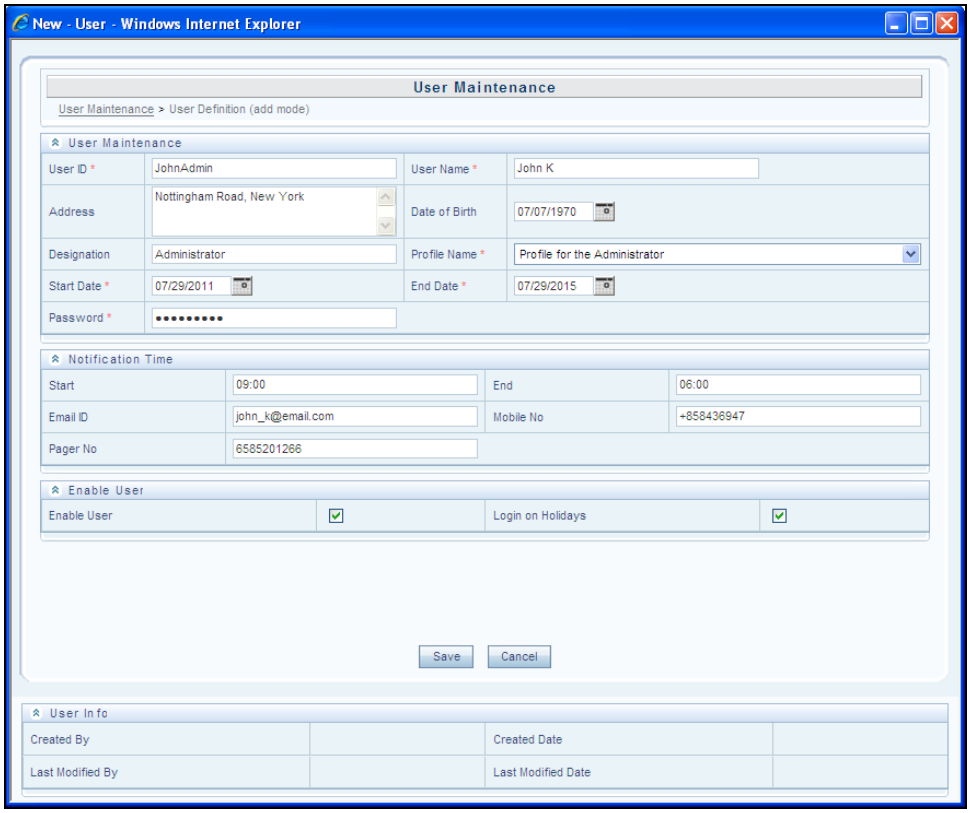
The *User Maintenance* screen displays user details such as User ID, Name, Profile Name, Start and End dates. You can also identify the user status if enabled, to access the Infrastructure system.

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.

#### 2.1.1.1 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.



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.<br>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 *Configuration* 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.<br>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.<br>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.

#### 2.1.1.2 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.

#### 2.1.1.3 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.

#### 2.1.1.4 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.

#### 2.1.1.5 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.

### 2.1.2 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.

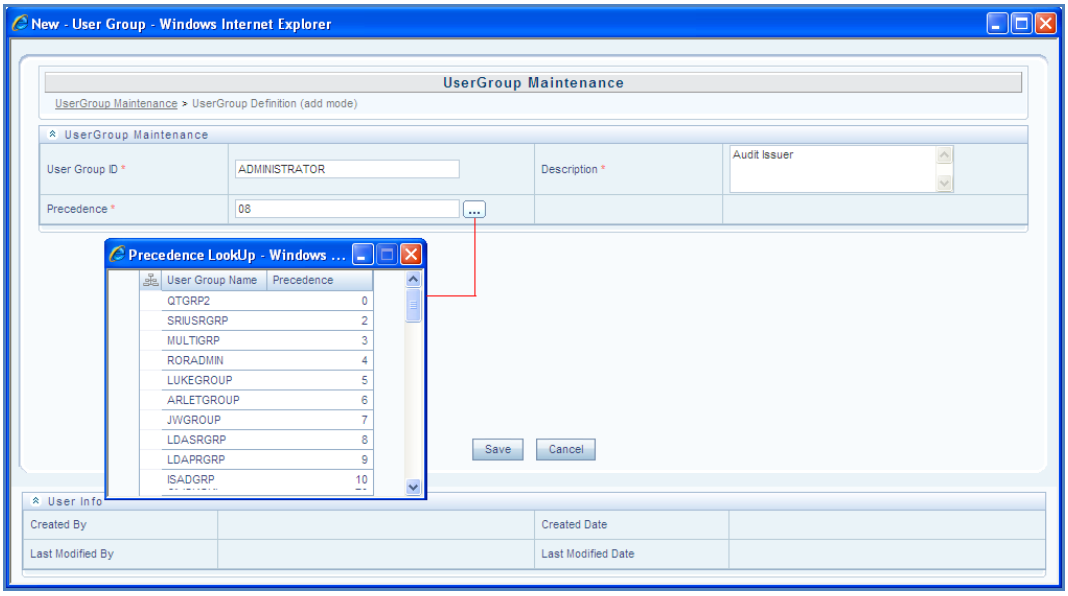
*UserGroup Maintenance* screen displays details such as User Group ID, Description, Precedence, and the number of Mapped Users.

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.

#### 2.1.2.1 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.

### 2.1.2.2 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.

#### 2.1.2.3 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.

#### 2.1.2.4 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.

### 2.1.3 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.

#### 2.1.3.1 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.

#### 2.1.3.2 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.

### 2.1.4 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.

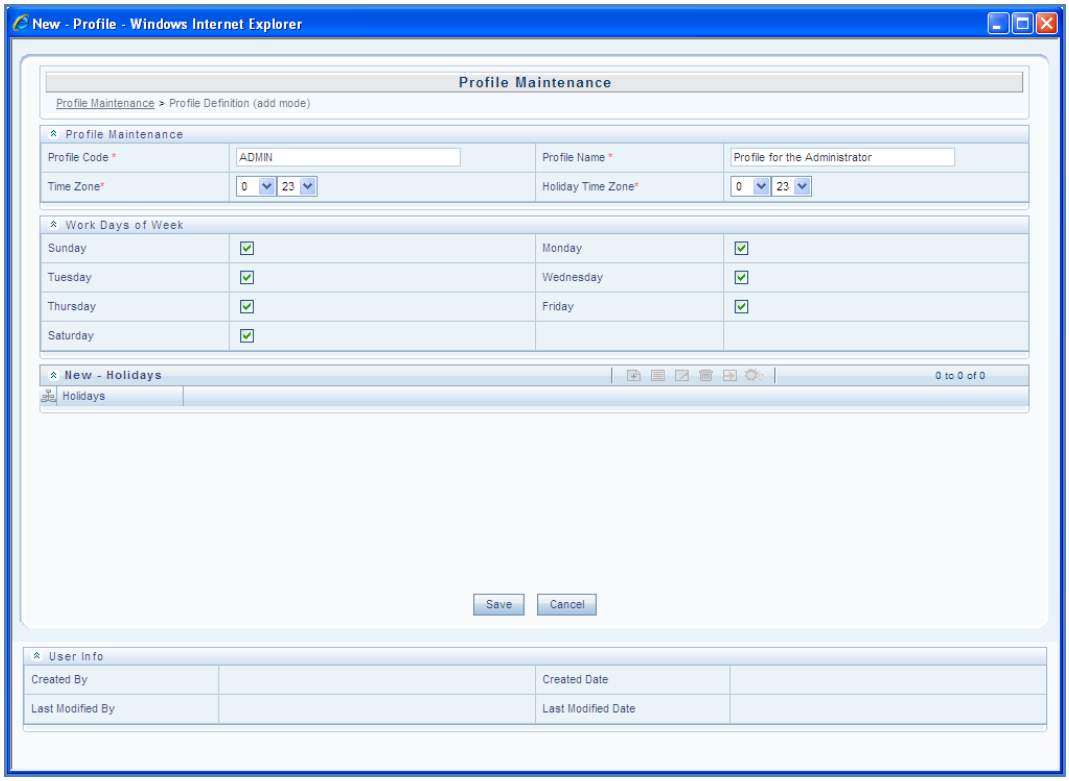
You can access Profile Maintenance by expanding **User Administrator** section within the tree structure of LHS menu.

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.

#### 2.1.4.1 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.




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. |

| Field | Description |
|---|---|
| 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.

#### 2.1.4.2 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.

#### 2.1.4.3 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.

#### 2.1.4.4 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.

#### 2.1.4.5 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.

### 2.1.5 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.

#### 2.1.5.1 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.

### 2.1.6 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/umapping 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 be 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.

#### 2.1.6.1 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.

### 2.1.7 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.

### 2.1.8 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 |
| 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 SuperUs 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 |

| ROLE CODE | ROLE NAME | ROLE DESCRIPTION |
|---|---|---|
| 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 |
| 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 |
| 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 |

| ROLE CODE | ROLE NAME | ROLE DESCRIPTION |
|---|---|---|
| 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 |

**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.

## 2.2 System Administrator

### 2.2.1 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 OBIEE servers namely;
  i. Weblogic Server
  ii. Oracle BI Server
  iii. Oracle BI Presentation Server
  iv. Oracle BI Java Host
- 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

### 2.2.2 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 6.1.0.0.0 is going to be installed. If not, SMPT 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 below.
- 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.

### 2.2.3 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.

## 2.2.4 Creating a New Access Control List

### 2.2.4.1 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.

### 2.2.4.2 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/xdb21sec.htm

### 2.2.4.3 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.

#### 2.2.4.4 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

#### 2.2.4.5 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.

**NOTE:** 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'.

**NOTE:** 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.

#### 2.2.4.6 Adding privilege to ACL

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

### 2.2.5 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.

#### 2.2.5.1 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>__MASKING_PRIORITY_KEY = HREF0023

Example value for <INFODOM>__ROLE_HIER = HREF0023

#### 2.2.5.2 Updating DIM_BASEL_CONFIGURATION table in Atomic Schema

EMAIL_DEFAULT_MSG_SUB = default email

EMAIL_DEFAULT_MSG_BODY= default body

Restart the OFSAAI servers.

### 2.2.6 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

**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 i.e. 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.

**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.

#### 2.2.6.1 List of Seeded Tables and Setup Tables used in Workflow

List of tables which needs to 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 needs to 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

#### 2.2.6.2 SEEDED TABLES

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

1. **WFM_LIST:** This table will define 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 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 will store 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 given below:

| N_NOTIF | N_WFM_MAS | N_NOTIF_STG_ST | N_WF_NOTI | V_NOTIF_ | V_NOTIF_DE |
|---|---|---|---|---|---|

| _KEY | TER_ID | ATUS_KEY | F_SEQ | NAME | SC |
|---|---|---|---|---|---|
| 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.

Sample Data for this table is given below:

| | |
|---|---|
| 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_COM |
|---|---|---|---|---|---|---|---|
| 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 given below:

| | |
|---|---|
| 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 given below:

| | 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 given section for more details.

    The Sample Data for the Masking_View_FFIEC table is given below:

| | |
|---|---|
| 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 given section 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 given below:

| 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 given below:

| 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 given below.

| 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 |

### 2.2.7 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 given below:

| 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).

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. Select the hierarchies HREF0023 and HREF0024. The sample name given for these hierarchies are “User Role” and “User Group”.

v. Enter the following details: Entries for Description, Effective From and Effective To.

**NOTE:** DO NOT select “Read Only” and “Generate Hierarchy Security”.

vi. Enter the Database Entity Name as ROLE_USRGROUP_MAP.

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

vii. Comments to the New Entry can be left blank. Click Save Definition as new version. The Version Description field can be left blank.

viii. Click Save. A new Mapper is created in the Mapper List and the table ROLE_USRGROUP_MAP is created in the mapped Atomic Schema.

ix. Select this Mapper and click Mapper Maintenance. The two selected hierarchies are displayed along with the Data.

x. Select the nodes and then click Save Mapping.

xi. Select the nodes and then click Save.

xii. 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.

xiii. Click View Mapping. It helps the Administrator to view the existing Mapping if any.

xiv. After the mapping is completed click **Save**.

xv. Click **Close** to close the screen.

xvi. Administrator must verify the mapping entries in **ROLE_USR_GROUP_MAP** table.

**NOTE:** In case the Admin doesnot setup the tables as mentioned in the Guide, the Default configuration as done through AAI will be picked up from the Config Schema and the corresponding User – Role configuration will be used for notifying the Users for Mail Utility.

### 2.2.8 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.

#### 2.2.8.1 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 gird record.

Sample Data for MASKING_VIEW_FFIEC is given below.

| | |
|---|---|
| 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 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 |

Admin Guide
January 2014
Oracle Financial Services Basel Regulatory Capital Analytics V6.1.0.0.0

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 © 2014 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.