ORACLE

FUSION APPLICATIONS
HUMAN CAPITAL MANAGEMENT

Customizing Fusion HCM OTBI Security

ORACLE WHITE PAPER | JULY 2014

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

.

Introduction

This white paper is a guide on how to implement and customize security for Oracle Transaction Business Intelligence (OTBI) analysis for HCM applications. In this white paper we will:

1. Grant line managers and employees the ability to view OTBI analyses for Workforce Management, Profile Management, Performance Management, and Goal Management subject areas. They will not be able to create analysis. The procedure can also be used to grant access to other HCM subject areas.

2. Grant the ability to create analyses to a set of users by role or by name.

3. Grant the ability to administer BI and BI Publisher data models to specific users by name.

4. Create a mechanism to secure OTBI analyses and folders in the BI Catalog so that only line managers can see analyses written for line managers and employees can only see analysis for employees when accessing the catalog.

The example in this document is for a limited set of subject areas. The procedures in this document can be used to grant access to any and all HCM subject areas. This will be called out in the appropriate steps below.

This white paper applies to Fusion releases up to and including release 8.

There are several ways to implement this functionality. This document will cover one of the recommended methods. The document will require the use of supplemental material listed in the prerequisites section of this document. Using the published security documentation will help to provide insights and additional information. When a step requires the use of additional materials, the step will specify which materials, chapters and sections to use to understand or perform the step.

To understand the terms and concepts used in this document see **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document. Review **Chapter 1 An Overview of HCM Security in the Cloud**.

OTBI subject area enablement is performed through the duties and roles inherited by job or abstract roles. An explanation of these roles and duties can be found in the following documents listed in the prerequisite section of this document:

- **Securing Oracle HCM Cloud** see **Chapter 11 Specialized Security**
- **Understanding Fusion HCM OTBI Security white paper** see **4 Delivered HCM Job Roles, OTBI Duty Roles and Reporting Data Roles**

Prerequisites

The materials below will be recommended or required while performing the steps in this document. It is recommended that you review the materials prior to performing the steps.

Securing Oracle HCM Cloud
Oracle Cloud Documentation Portal: http://docs.oracle.com/cloud.

Under Application Services, Global Human Resources link
In Global Human Resources Cloud page, tab Cloud Books.
In Security section, click Securing Oracle HCM Cloud.

Cloud Books and On Premise Books in the Oracle Cloud Documentation portal contain a series of security documents that are helpful in understanding Fusion HCM security.

Understanding Fusion HCM OTBI Security white paper
Oracle Applications Customer Connect: http://appsconnect.custhelp.com/pages/home
Use the search option in Customer Connect to find the "Understanding Fusion HCM OTBI Security" posted by Ling Xiang

Role Customization Best Practices recorded webcast
Oracle Applications Customer Connect: http://appsconnect.custhelp.com/pages/home
Use the search option in Customer Connect to find the "Role Customization Best Practices" event posted by Fred Voltmer.

Step 1 Create New Custom Fusion HCM Abstract Roles

In this example we are creating one new abstract role for line manager reporting and one for employee reporting. Having separate abstract roles makes it easier to implement different privileges to employees and line managers. You can add OTBI reporting functionality to your existing custom roles. If you opt for this option, skip this step and move to the next step of adding new duties to the roles.

*Never modify delivered job or abstract roles unless advised to by Oracle. For instructions on how to create a custom copy of delivered roles, see **Role Customization Best Practices** recorded webcast and **Securing Oracle HCM Cloud** documentation listed in prerequisites section of this document.*

Follow the procedure in **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document. See **Chapter 9 Customizing Security**> **Creating Custom Job or Abstract Roles** > **Creating a Custom Job or Abstract Role: Procedure**

Create one abstract role for line managers and another abstract role for employees. See example of the line manager abstract role in screenshot below.

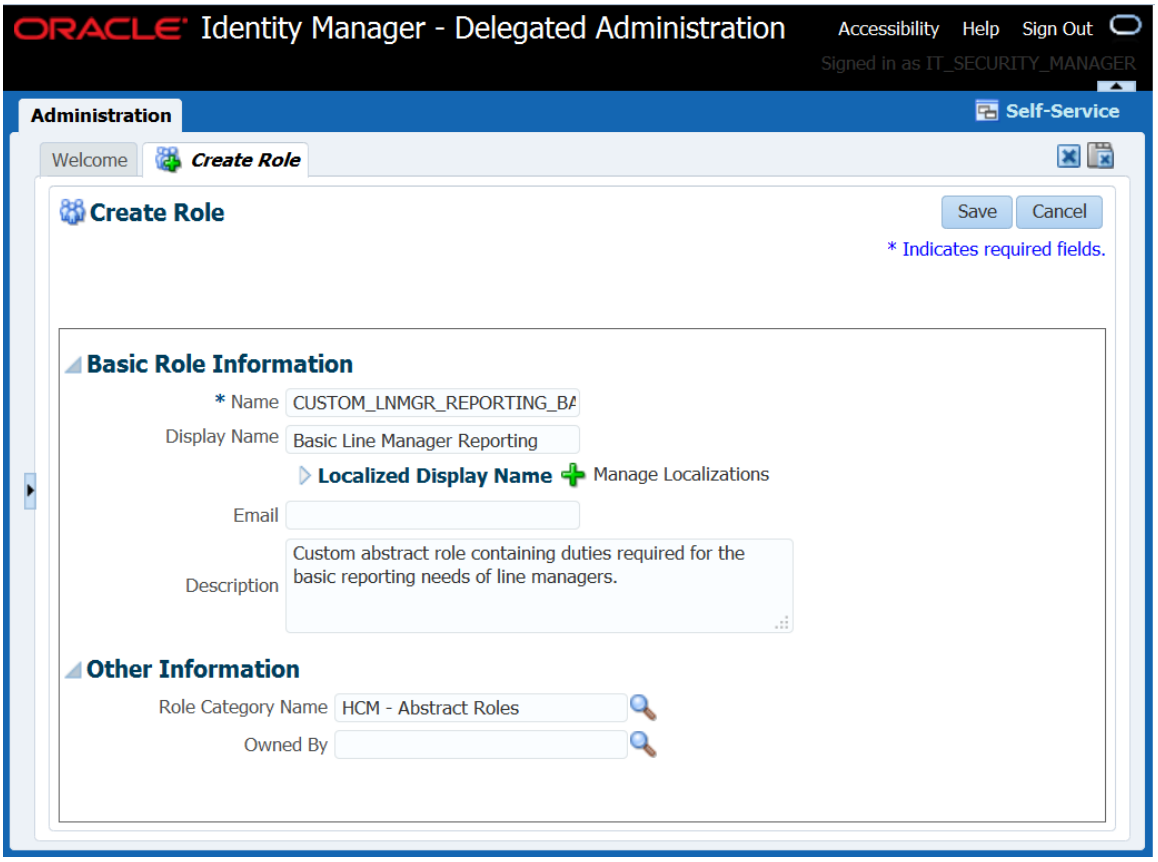


Figure 1. Example of creating the new line manager abstract role.

Important!: The Role Category for the abstract role must be "HCM – Abstract Roles".

Step 2 Add Transaction Analysis Duty Roles to the Abstract Roles

Follow the procedure in **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document. See **Chapter 9 Customizing Security** > **Creating Custom Job or Abstract Roles** > **Adding Duties to a Job or Abstract role: Procedure.**

In the procedure, you will open an External Role. Open the line manager abstract role created in step 1 or if you are modifying an existing custom abstract role, open your existing custom abstract role instead.

During the procedure you will map duties to your role. When in the Map dialog box, search for duties using the following criteria: in the **Application** field, select **hcm,** in the **Display Name** field select **Ends with** and in the text box enter the text: **Transaction Analysis Duty.** Select search to see the hcm duties that manage HCM OTBI subject areas. Select the following duties and click Map Roles:

- Goal Management Transaction Analysis Duty
- Performance Management Transaction Analysis Duty
- Workforce Profile Transaction Analysis Duty

» Workforce Transaction Analysis Duty.

Click on the Map icon in the Application Role Mapping tab again. When in the Map dialog box, search for duties using the following criteria: in the **Application** field, select **obi,** in the **Display Name** field select **Ends with** and in the text box enter the text: **Transaction Analysis Duty.** Select search to see the obi duties that manage all OTBI subject areas. Select the following duties and click Map Roles:

» Goal Management Transaction Analysis Duty
» Performance Management Transaction Analysis Duty
» Workforce Profile Transaction Analysis Duty
» Workforce Transaction Analysis Duty.

Open the employee abstract role created in step 1 or if you are modifying an existing custom abstract role, open your existing custom abstract role instead. Add the same hcm and obi duties to the employee abstract role.

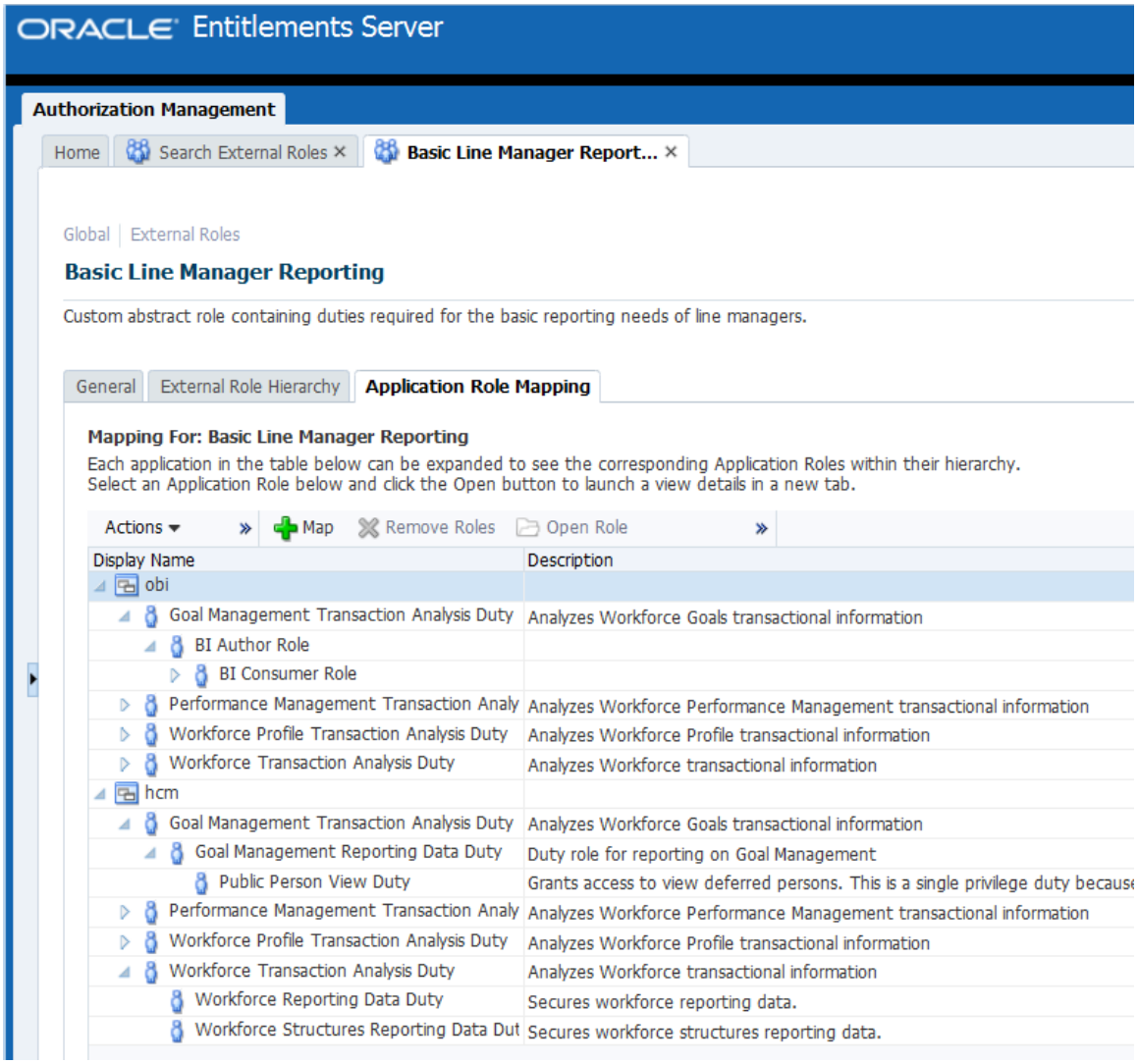


Figure 2. The Application Role Mapping tab with obi and hcm duties.

All HCM subject areas are supported by the hcm Workforce Transaction Analysis Duty. Under most conditions, this duty should be added for any role having access to any HCM OTBI subject area. See explanation below.

Brief overview of the Transaction Analysis duties

Expand the duty trees to see all of the sub duties and roles in each of the duties. The hcm duties contain Reporting Data and View Duties while the obi duties contain BI Roles.

The hcm duties control data security within the subject areas. Each application has an hcm duty role for the data managed by their transactions. A subject area may have data from more than one application. In order to use all functionality within the subject area, more than one hcm duty may be required. For example, the Goal Management subject areas have dimensions and facts from Goal Management (Performance Goals, Goal Plans, etc) and they have dimensions from Workforce Management (Worker, Job, Department, etc). In order to view all data in the Goal Management subject areas both the hcm Goal Management Transaction Analysis Duty and the hcm Workforce Transaction Analysis Duty should be included. If the hcm Workforce Transaction Analysis Duty were missing, the user would be able to see goal information in analyses created with the Goal Management subject areas, yet the worker information (Worker Name, Manager Name, Department, etc) would be null.

The obi duties control the access to subject areas. Each application has an obi duty role tied to the subject areas for the application. If the user should only have access to Goal Management subject area analyses and not Workforce Management subject area analyses, the obi Goal Management Transaction Duty would be added and the obi Workforce Transaction Analysis Duty would not.

The hcm and obi duties do not affect the folders and attributes visible in the subject area. Users who have the ability to create analysis will see all folders and attributes regardless of security settings.

See **Understanding Fusion HCM OTBI Security white paper** listed in the prerequisites section for more information about OTBI duties.

Step 3 Change Duty Roles to View Analyses Instead of Create Analyses

In Release 8 and prior, the Transaction Analysis Duty roles are delivered with the ability to create analyses. In Step 3, we will restrict the duties to have only the ability to view saved analyses. This change will affect every job and abstract role that inherits these duties. In step 4 we will add the ability to create analyses directly to the roles that still require it.

Continuing from Step 2 where you added duty roles to the employee abstract role, in the Application Role Mapping tab of the abstract role click on the each duty role under obi and click open role.

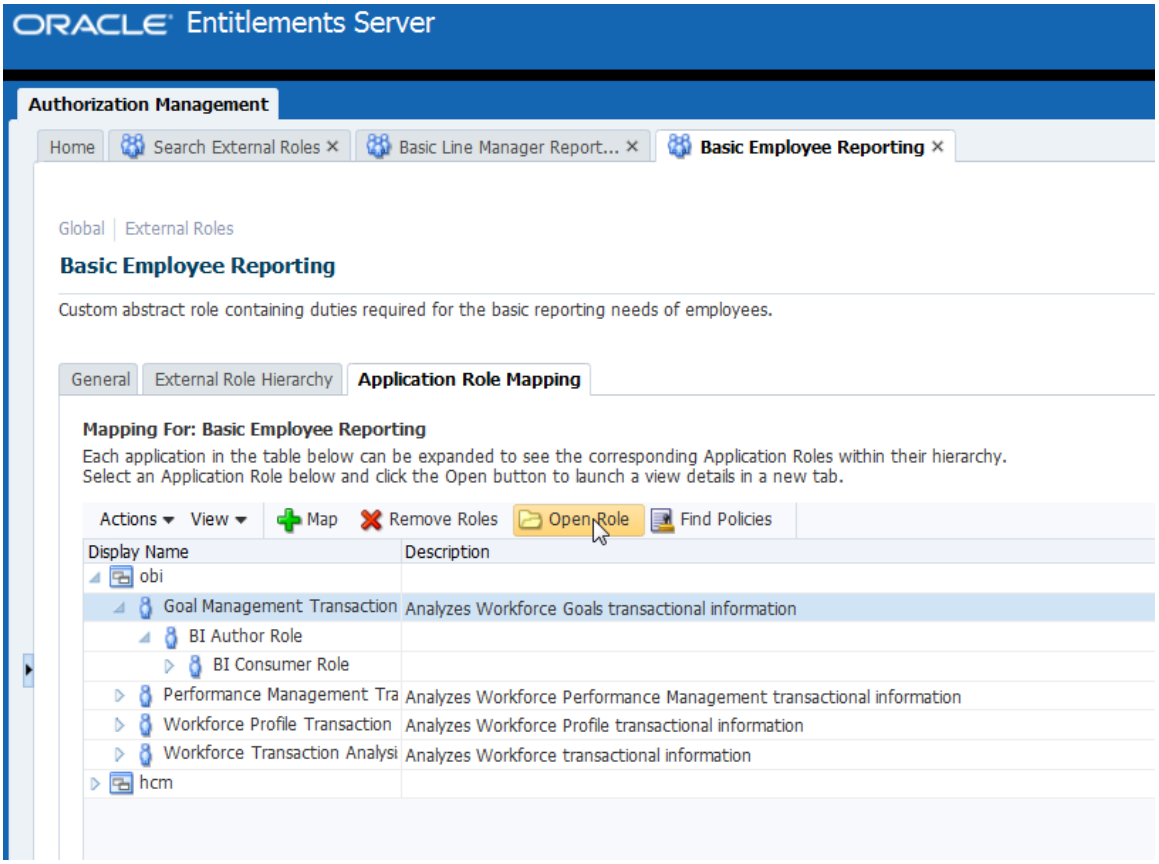


Figure 3. Opening the duty role.

Click on Application Role Hierarchy tab of the duty role and remove BI Author role. This will remove the BI Author and BI Consumer role nested within the BI Author role.

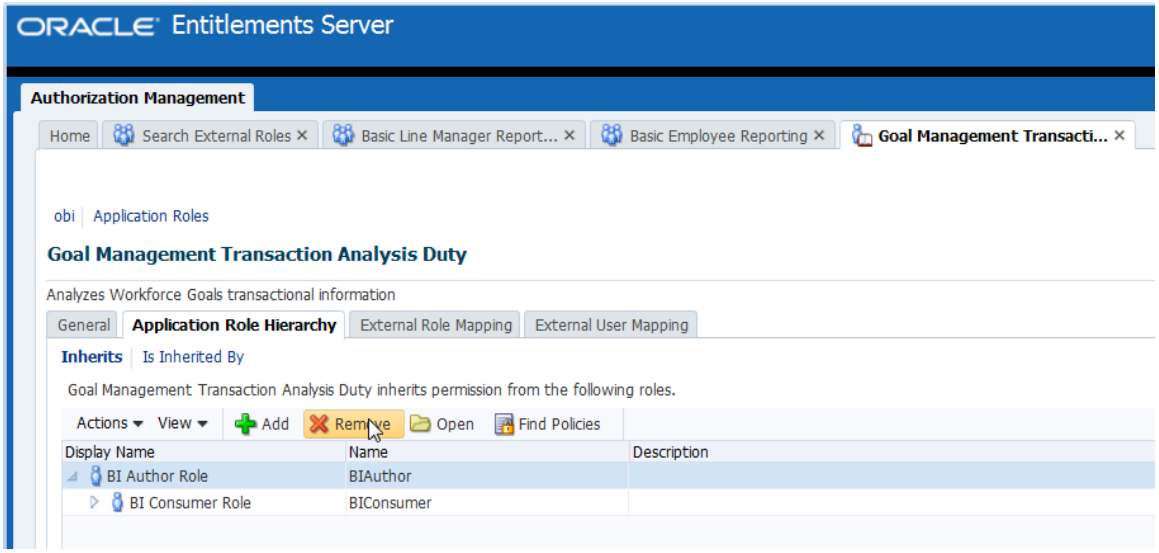


Figure 4. Removing the BI Author role from the Goal Management Transaction Analysis Duty.

Clicking on Add, search for Role Display Name starts with BI Consumer Role. Select the BI Consumer Role in the search results and select Add.

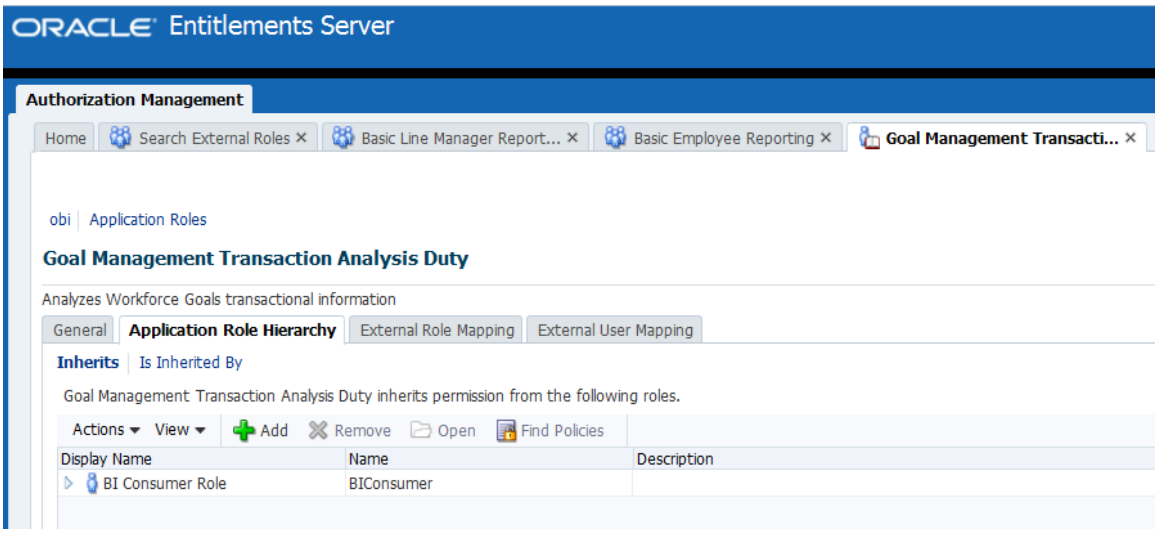


Figure 5. BI Consumer role added to the Goal Management Transaction Analysis Duty.

Perform this procedure for each obi Transaction Analysis Duty. Since these changes will affect all job or abstract roles that inherit these duties, you do not need to perform these steps on the duties in the abstract line manager role.

Important! If a user inherits the BI Author role through any other role or duty, the user will be able to create analysis with all subject areas managed by any of the duties they've inherited through any job or abstract role. You must remove the BI Author role from every job role, abstract role, and any duty the user inherits. See troubleshooting section for more information.

Step 4 Grant Ability to Create Analyses to Roles That Need It

There are several ways to perform this step. In this example, we will continue from Step 3 and perform the action from the duty roles page within our new employee abstract role. Each obi Transaction Analysis Duty role should already be opened in a separate tab. For each open duty, click on External Role Mapping tab in the duty page to see the roles that inherit the duty.

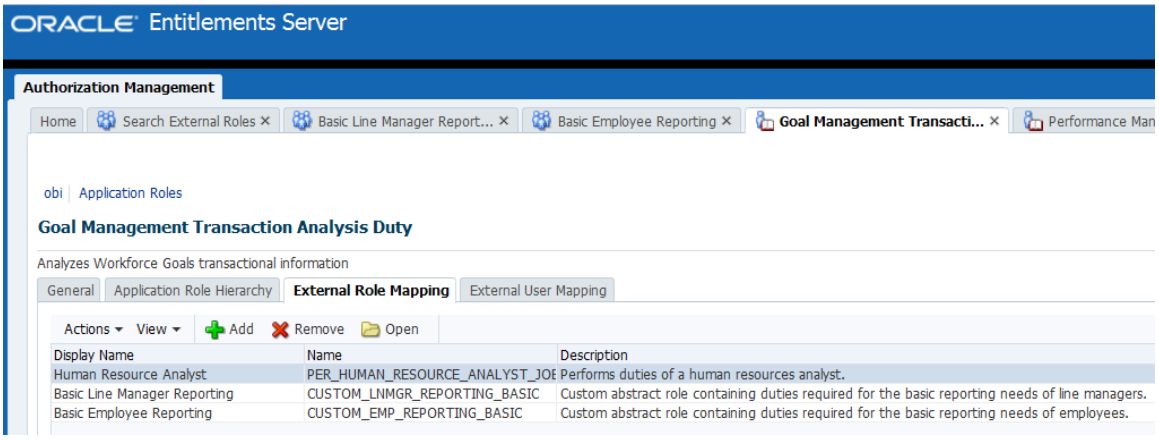


Figure 6. External role mapping of the Goal Management Transaction Analysis duty.

In our example, the Goal Management Transaction Analysis Duty is inherited by the Human Resource Analyst role and our new custom line manager and employee abstract roles. The Human Resource Analyst role requires the ability to create analyses, so we must add the BI Author role to the Human Resource Analyst job role.

Select the role Human Resource Analyst role and click on the Open icon. The Human Resource Analyst role will open.

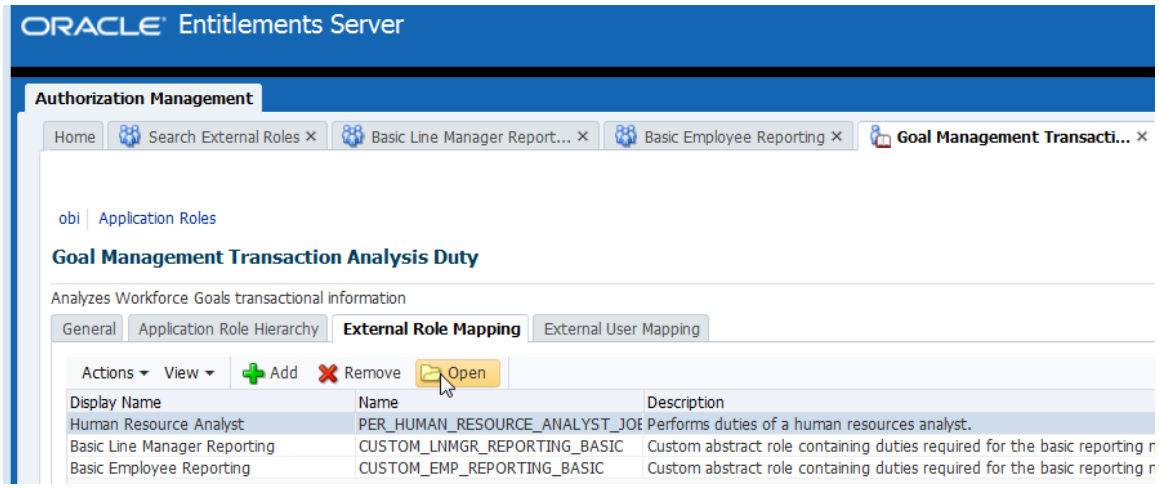


Figure 7. Opening the Human Resource Analyst job role from the duty page.

Click on Application Role Mapping tab and click on the Map icon to map Application Roles. When the Map dialog box, search for the BI Author role using the following criteria: in the **Application** field, select **obi,** in the **Display Name** field text box enter the text: **BI Author** and click on search. Select the BI Author role in the search results and click Map Roles.

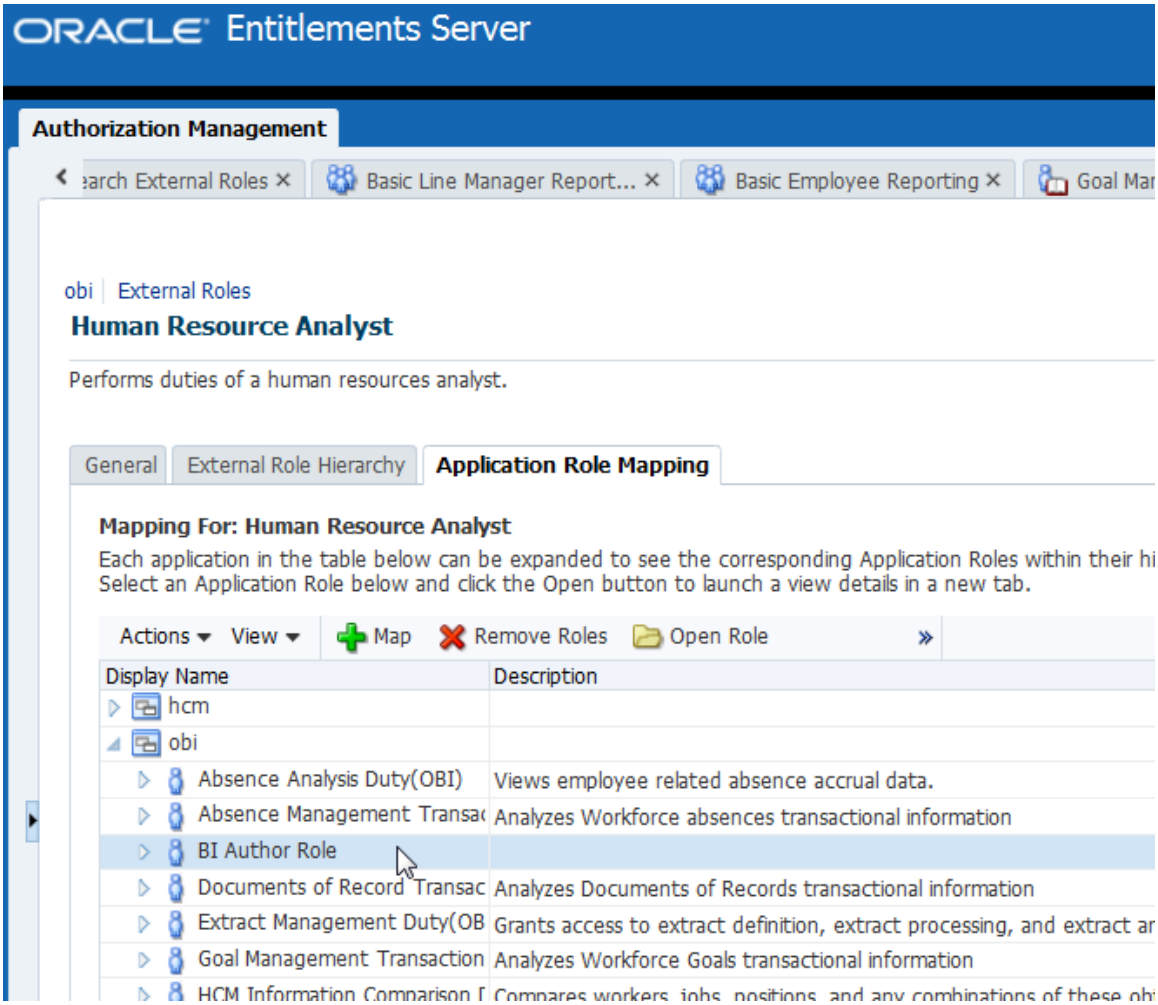


Figure 8. The BI Author role added to the Human Resources Analyst job role

Check each Transaction Analysis Duty.

In our example, the Workforce Transaction Analysis Duty is inherited by the Human Resource Analyst role, the delivered Line Manager abstract role and our new abstract roles. We've already added the BI Author role to the Human Resource analyst role and none of our other roles require the ability to create analysis, thus there are no changes required for the roles inheriting this duty.

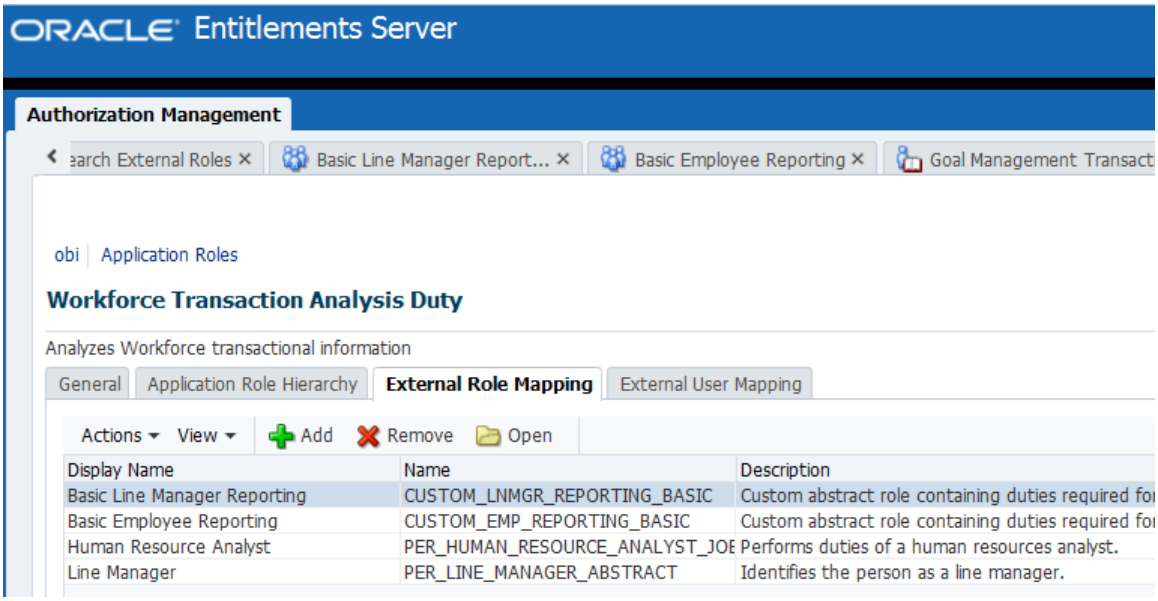


Figure 9. External role mapping of example Workforce Transaction Analysis Duty.

Step 5 Manage BI Catalog Permissions Using OBI Application Roles

There is more than one way to secure analyses and folders in the BI Catalog. One useful technique is through the use of OBI Application roles in folder and analyses permissions. A user having the BI Administrator role or who is an owner of a folder or analysis can view or set permissions.

To change or view permissions, navigate to the folder or analyses in the BI Catalog, select more and select Permissions from the list of more options.

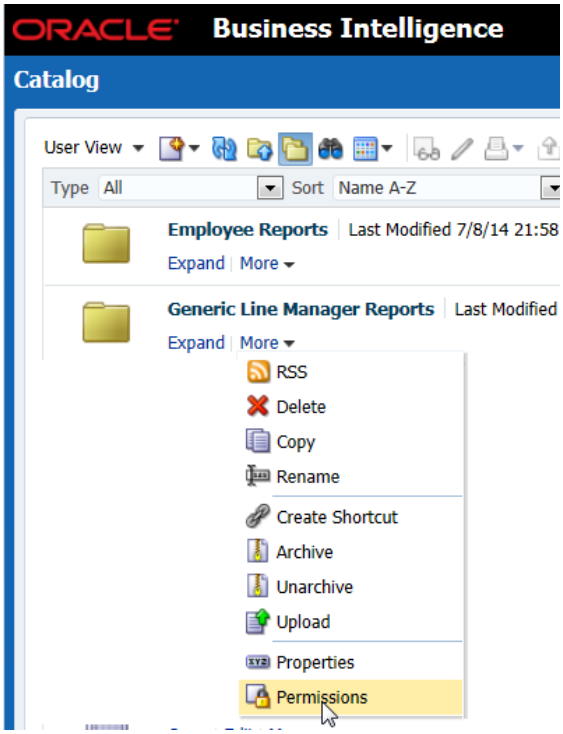


Figure 10. Permission option in the list of more options for a folder in the BI Catalog.

The default permissions for new folders and analyses allow BI Administrators and BI Authors to have full control of the folder or analyses, and BI Consumers can only view folders and analyses.

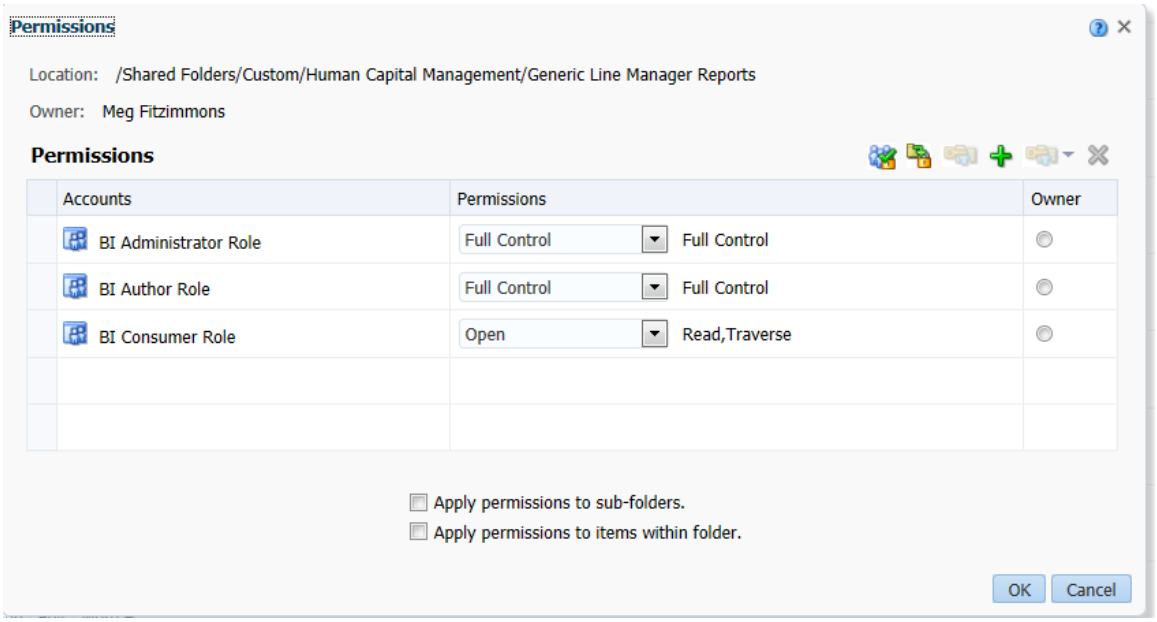


Figure 11. Default folder permissions.

To add additional permissions, click on the Add User Roles (plus icon) above the permissions table. The Add Application Roles, Catalog Groups and Users dialog box opens. The available options are Application Roles, Catalog Groups, Users and All. We will create application roles which we will add to our abstract roles so that our folders and analyses are secured by the abstract roles assigned to users.

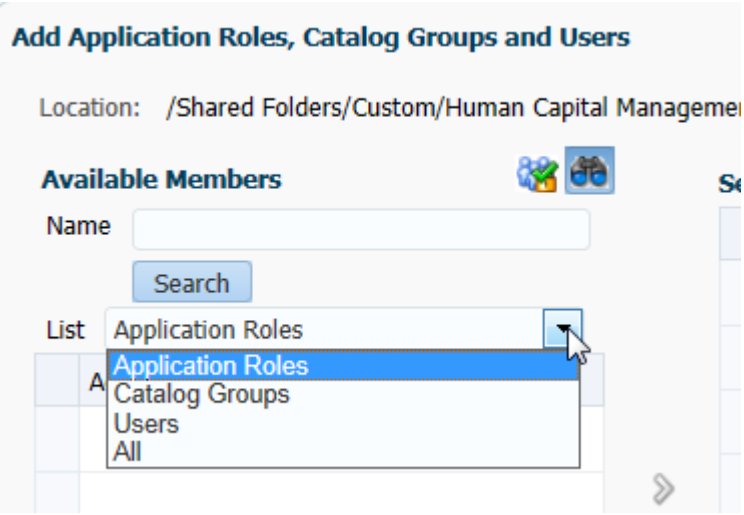


Figure 12. Add Application Roles, Catalog Groups and Users dialog.

Create obi Application Roles by signing in to Oracle Fusion HCM with the IT Security Manager job role and follow these steps:

1. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.
2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task. Application roles are managed through Duties because they are Oracle Fusion Application Duties.

   The Oracle Entitlements Server Authorization Management page opens.
3. In the Application Name section on the Home tab of the Authorization Management page, select **obi**.
4. In the Application Roles section, click New.
5. Give the role a display name, a role name and description indicating that this role is for line managers. Leave the role category field blank. See example below.
6. Save.
7. Click Home and repeat the steps to create the employee application role used for BI Catalog permissions.

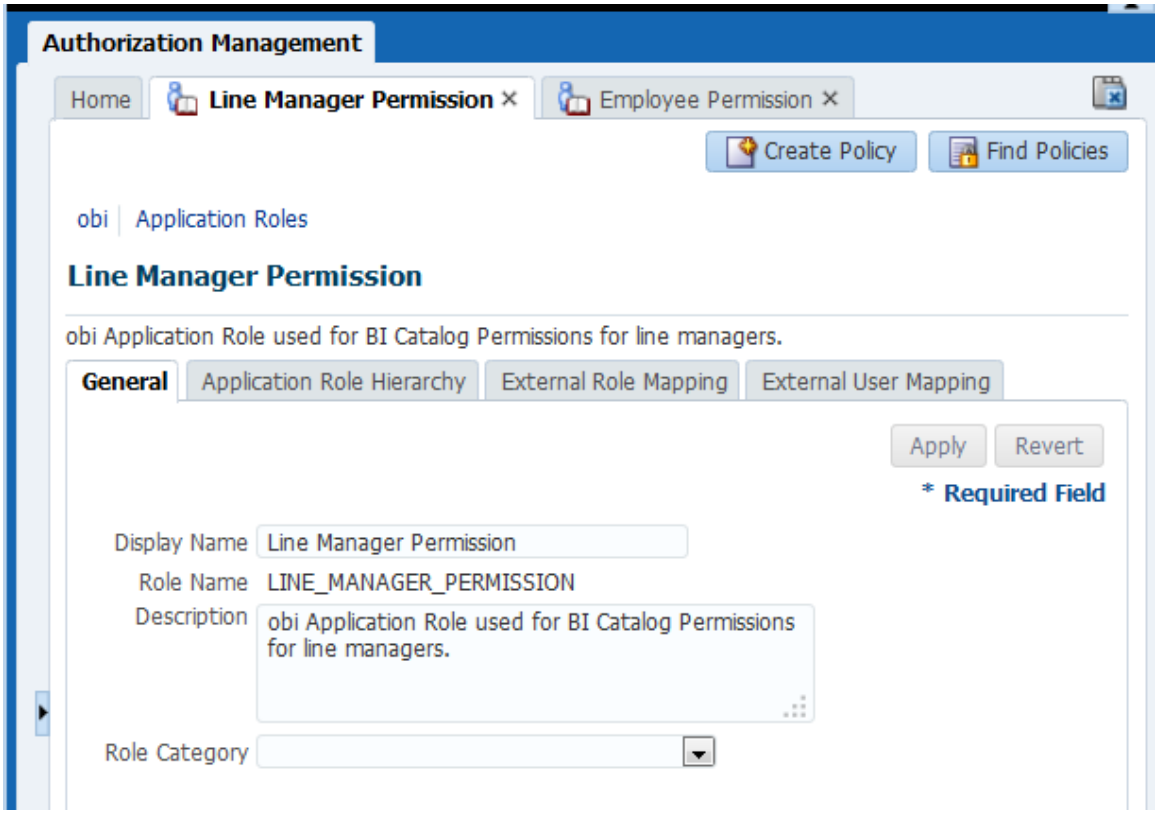


Figure 13. Line Manager Permissions obi Application Role.

Add the new application roles to the new custom abstract roles created in Step 1 by following these steps.

1. While in the Oracle Entitlements Server Authorization Management page, click on the Home page tab to return to the home page.
2. In the Application Name section on the Home tab of the Authorization Management page, select **hcm**.

Tip: If you don't select hcm, then you can't search for HCM duty roles.

3. In the Search and Create section, click Search - External Roles.
4. In the Display Name field of the Search - External Roles page, search for the job or abstract roles used for line manager and employee reporting.. The roles in this example are Basic Line Manager Reporting and Basic Employee Reporting.
5. In the Search Results section, select each role and click Open Role.
6. On the role page, click the Application Role Mapping tab.
7. Click Map.

   The Map Application Roles to External Role dialog box opens.

   a. In the Application field, select obi.

   b. In the Display Name field, enter the name of the role that you want to add. For example, while in the line manager abstract role, we will search for the new Line Manager Permission Application Role.

c. Click Search.

8. Select the role in the search results and click Map Roles.

   The application role (duty role) that you added now appears in the obi folder on the Application Role Mapping tab.

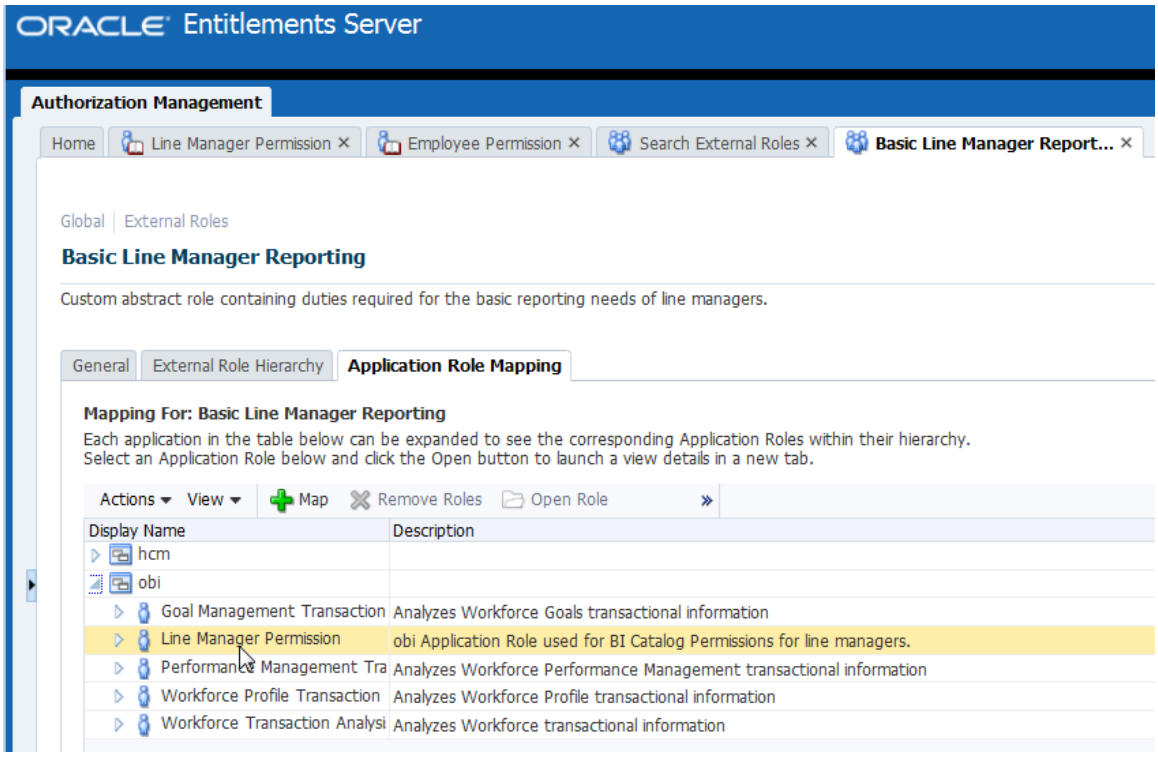


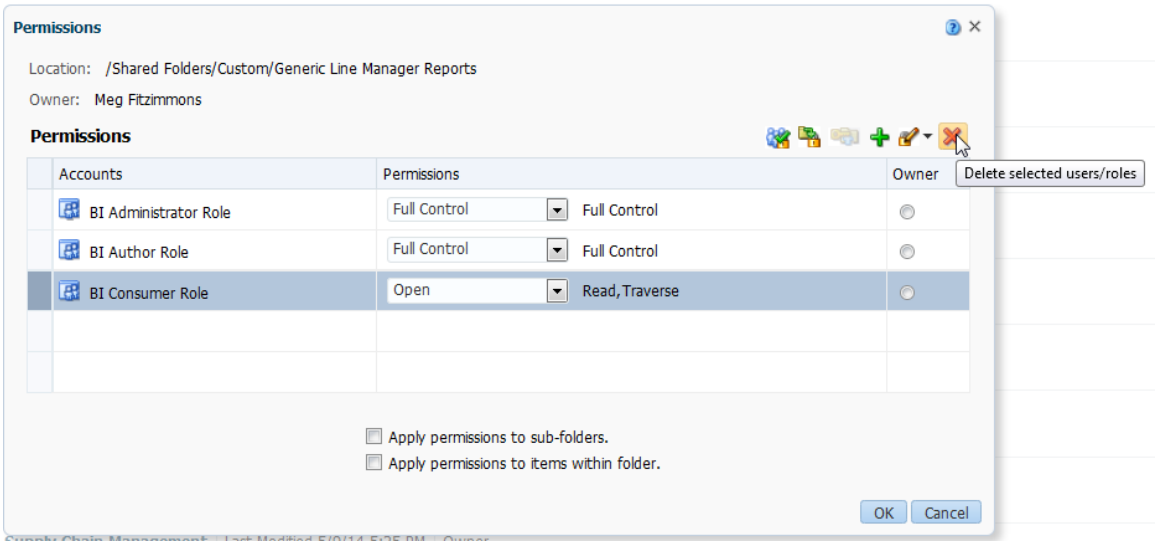
Figure 14. new obi application role (duty role) for line manager permissions added to Line Manager Reporting abstract role.

9. Repeat steps to add the employee obi application role (duty role) to the employee reporting abstract role.

Change permissions in the BI Catalog to use the new obi Application Roles.

Navigate to a folder or analyses in the BI Catalog as either a BI Administrator or as a BI Author owning the catalog folder or analyses. On the folder or analyses select more and select Permissions from the list of more options. See Figure 10. Permission option in the list of more options for a folder in the BI Catalog.

In the Permissions dialog, remove the BI Consumer Role from the Permissions list by clicking on the BI Consumer Role in the Permissions table and clicking on the Delete selected users/roles red X icon.



Add users/roles by clicking on the green plus (Add users/roles) icon. The Add Application Roles, Catalog Groups and Users dialog opens. In the Name field enter the display name of the obi Application role applicable to this folder or analyses and click Search. Select the role in the Accounts table, select Set Permission to Open and shuttle the account to the Selected Members area. For example, in a folder intended for line managers, we've selected the Line Manager Permission application role created in prior steps. We set Permission to Open and we've shuttled the account over to Selected Members.

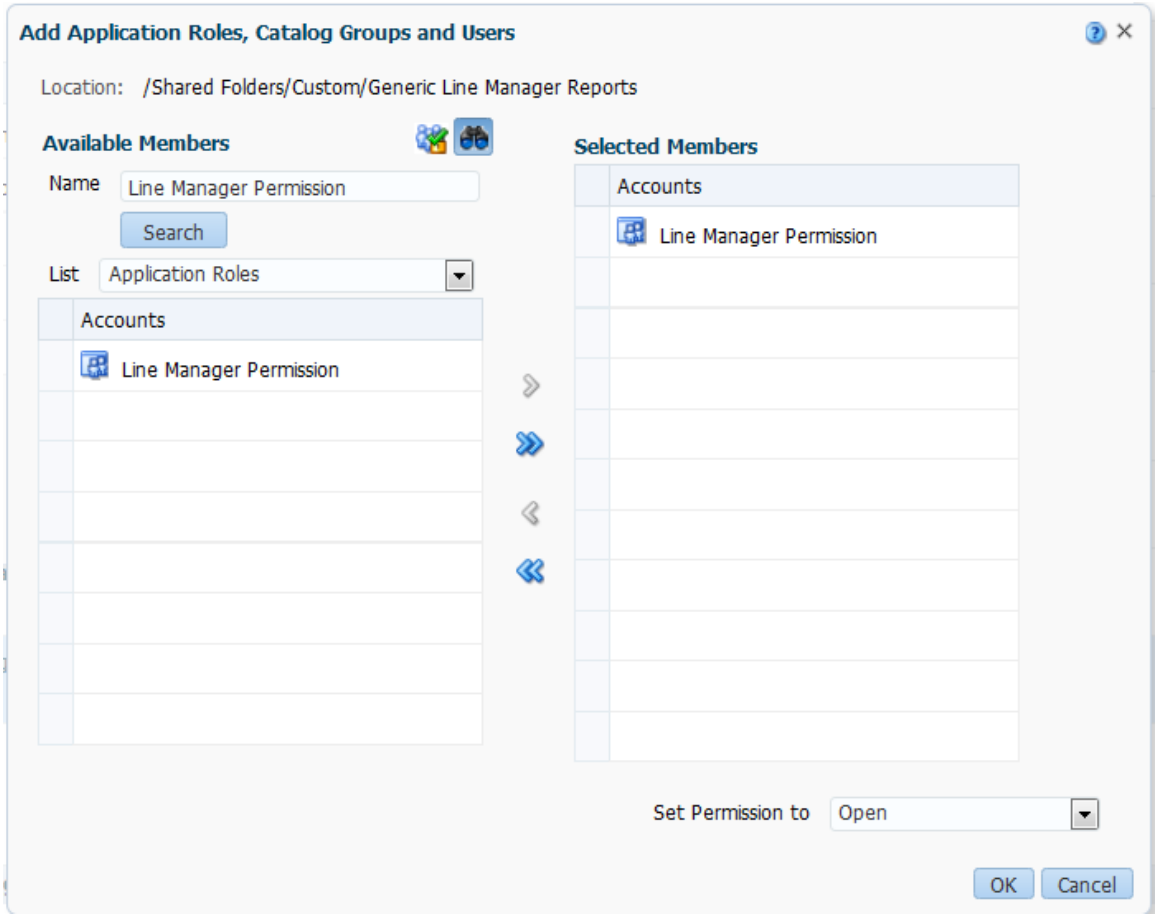


Figure 15. Line Manager Permission application role as Selected Member.

Click Ok to close the dialog. The application role appears as an account in Permissions. Click Ok to close the Permissions window.

The following Permissions indicate that the users who are BI Administrators or BI Authors have full control over the folder, while users with the Line Manager Permission role will have permission to open the folder.

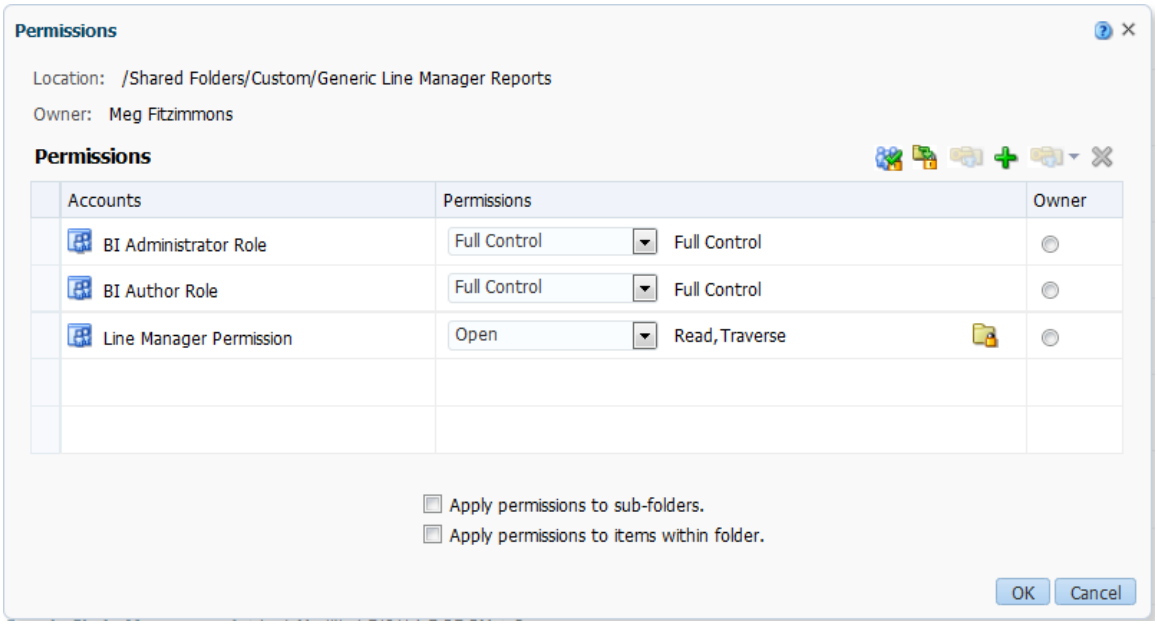


Figure 16. New Permissions for folder.

Step 6 Run Retrieve Latest LDAP Changes Process

See **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document > **Chapter 10 Synchronizing User and Role Information with Oracle Identity Management**.

The process exposes the new abstract roles and any changes to hcm duty roles to Fusion HCM. Refresh the scheduled process search results until the process status is “Succeeded”. You may then proceed to Step 7.

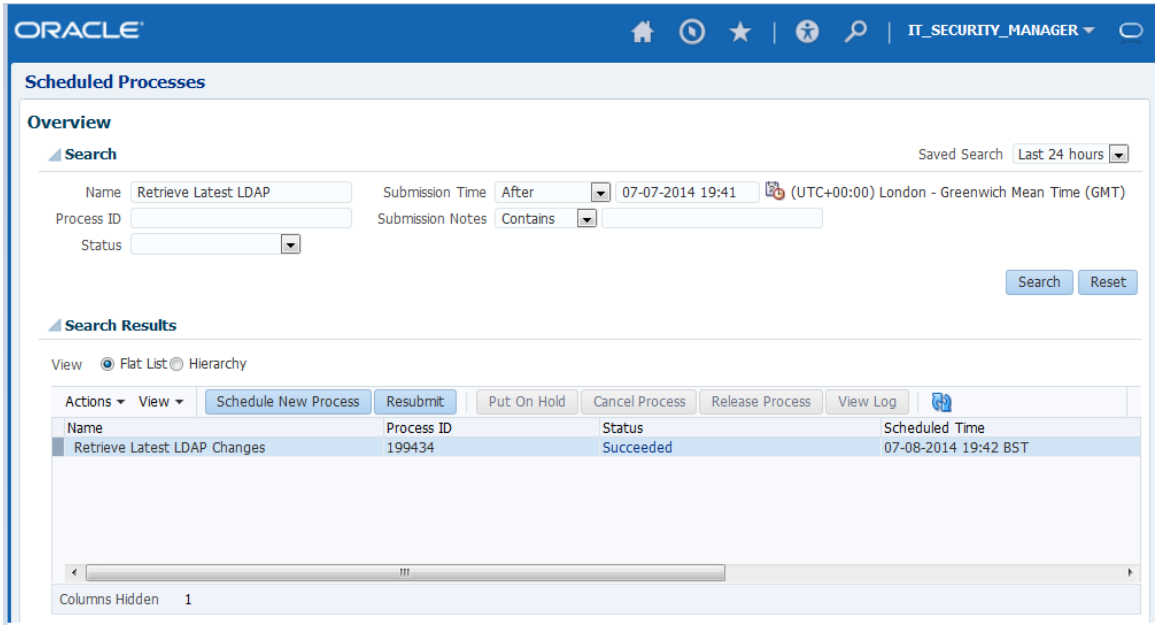


Figure 17. The Retrieve Latest LDAP Changes process has succeeded.

Step 7 Generate Security Policies using Data Roles

For any new job or abstract role or change in hcm duties in a job or abstract role, security policies must be generated using a data role.

Sign in to Oracle Fusion HCM with the IT Security Manager job role and follow these steps:

1. Open the Setup and Maintenance work area (Navigator - Tools - Setup and Maintenance).
2. On the All Tasks tab of the Overview page, search for and select the Manage Data Role and Security Profiles task.
3. In the Search section of the Manage Data Roles and Security Profiles page, enter the name of the role used for line manager reporting. In our example, this would be the new ”Basic Line Manager Reporting” abstract role.
4. In the Search Results section, select the role and click Edit.
   The Assign Data Role: Role Details page opens.
5. Click Next to traverse to the Security Criteria Train stop.
6. Enter security criteria applicable to a line manager, allowing line manager’s to view people in the manager hierarchy. The Security Criteria sections in the Security Criteria page will vary depending on the duty roles inherited by the role you have selected. If you are modifying an existing role, the security criteria may be different than shown in the example. See example below.

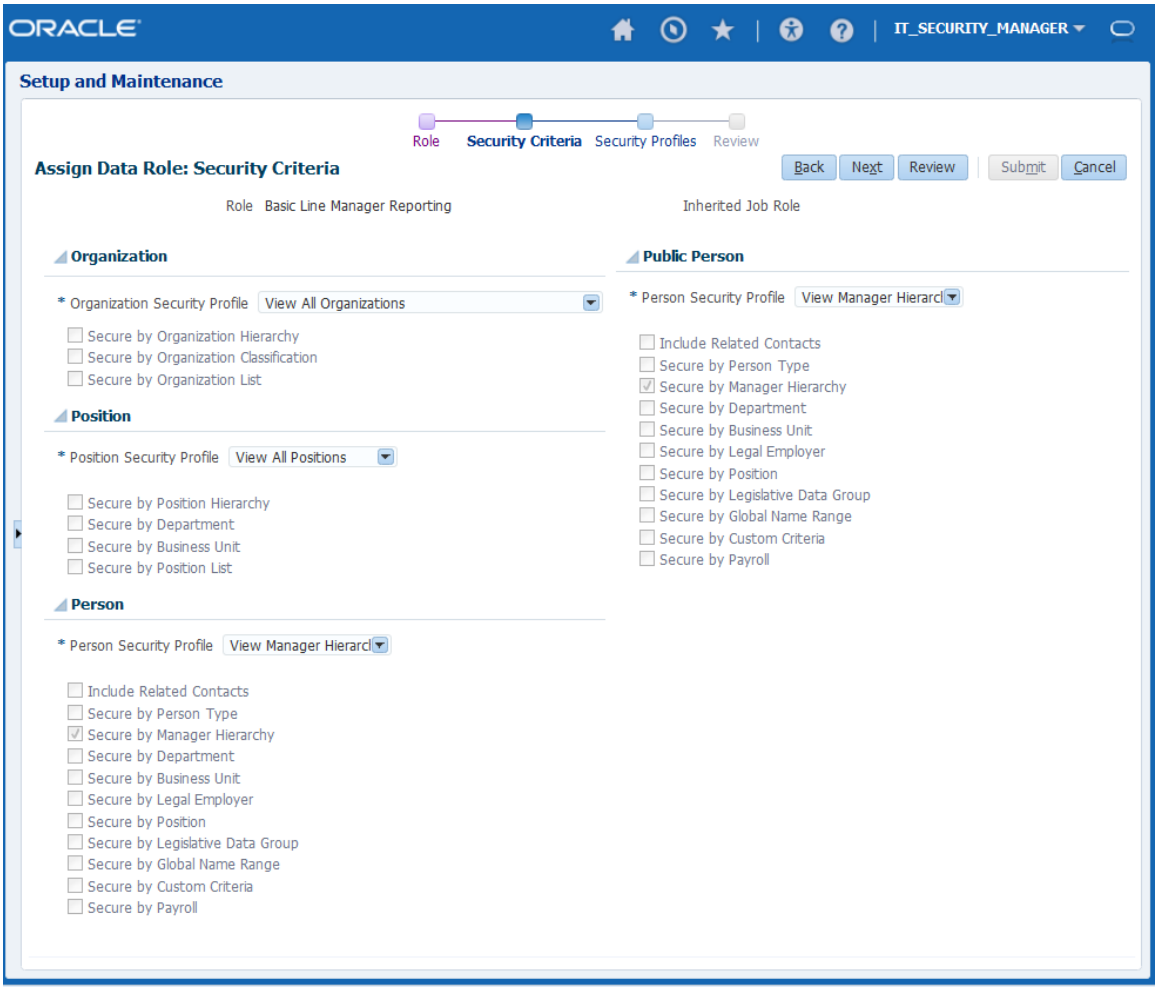


Figure 18. Security Criteria for custom Basic Line Manager Reporting abstract role.

7. Click next through the train stops until you are in the Review Page.
8. Click Submit.
9. Repeat the procedure for the Basic Employee Reporting abstract role, allowing employees to view their own record. See example below.

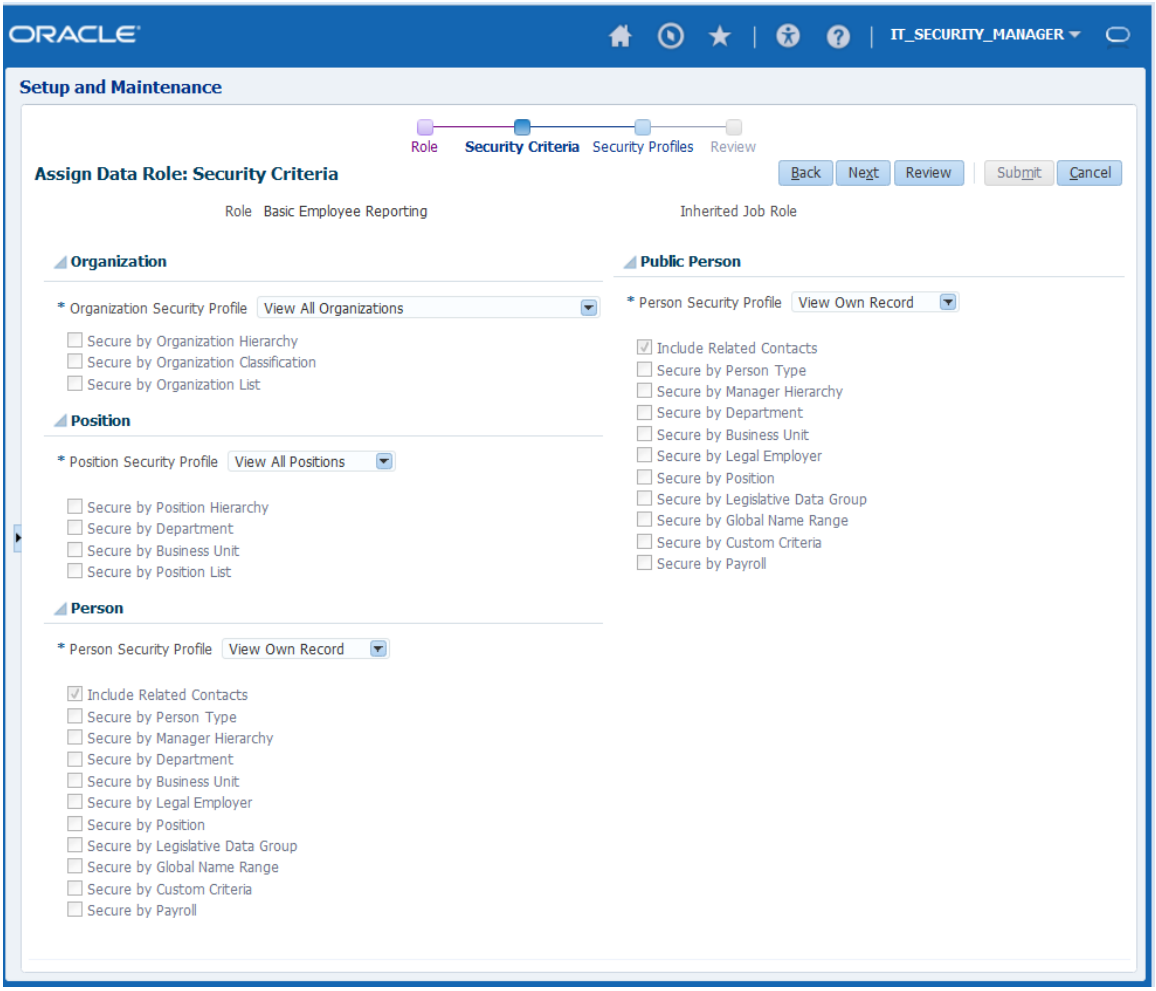


Figure 19. Security Criteria for custom Employee Reporting abstract role.

For more information see **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document > **Chapter 7 Creating HCM Data Roles**.

Troubleshooting Tip: If you run into an error, change the Delegation Allowed setting.

Step 8 Create a Role Mapping to Provision the Role to Users.

We will first manually give our new abstract role to test users. When we've tested security and ensured that it is correct, we will then give the roles to the rest of the line managers and employees.

If you are familiar with security and have an existing mapping that you use for your line managers, you can add the new role for line manager reporting to your existing line manager role mapping.

Follow the steps in **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document > **Chapter 6 Provisioning Roles to Application Users** > **Creating a Role Mapping: Procedure**.

In this example, we are mapping our new Basic Line Manager Reporting abstract role to users who are Managers with Reports using the Managers with Reports condition. We do not yet allow delegation, auto provisioning or users to request the role.

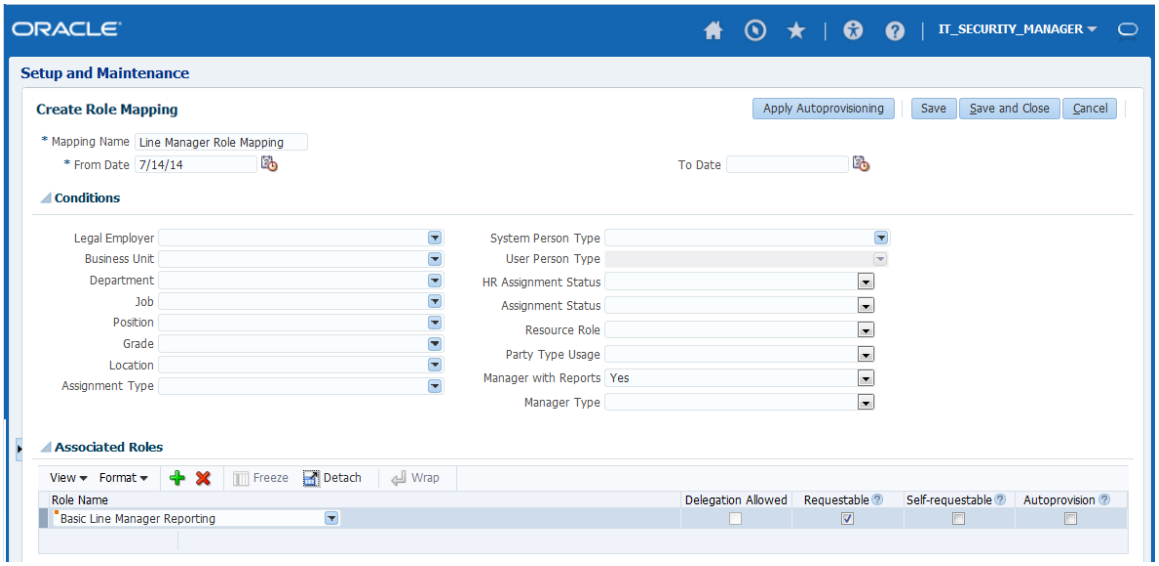


Figure 20. Example of role mapping for line managers. In the Conditions section, the Manager with Reports field is set to "Yes" and in the Associated Roles, only the Requestable checkbox is checked. No other options are allowed for the role.

Be sure to uncheck the autoprovision flag until you are ready to provision the role to all users.

Repeat for the new employee abstract role. In this example, we are mapping the Basic Employee Reporting abstract role to users who are employees using the System Person Type condition. We do not yet allow delegation, auto provisioning or users to request the role.

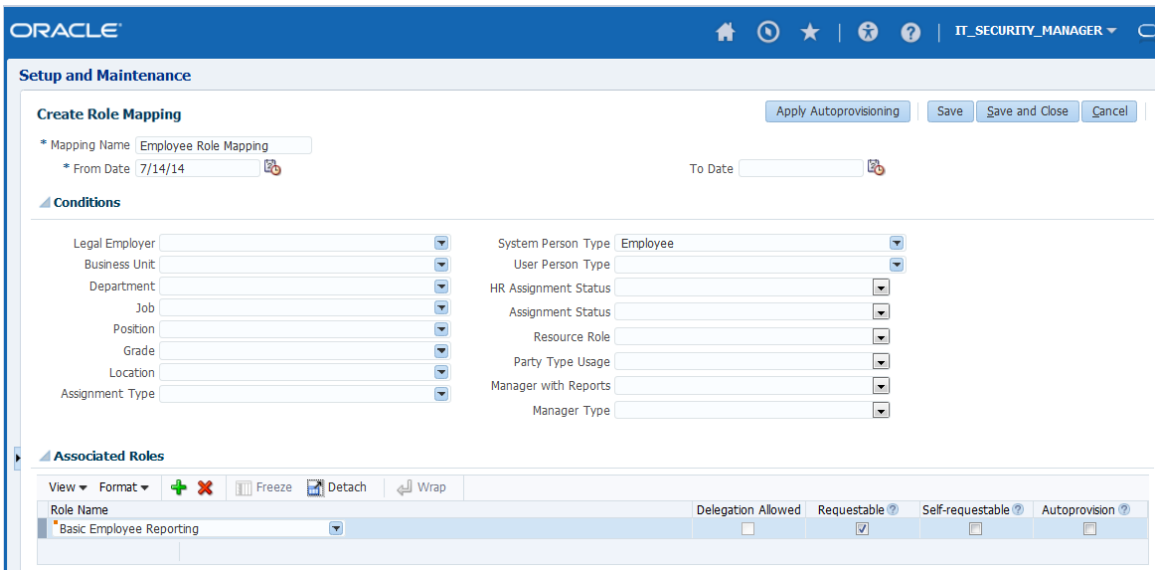


Figure 21. Example of role mapping for employees. In the Conditions section, the System Person Type field is set to "Employee" and in the Associated Roles, only the Requestable checkbox is checked. No other options are allowed for the role.

Step 9 Add Data Role to Test Users

Follow the procedure in **Securing Oracle HCM Cloud** documentation listed in the prerequisites section of this document > **Chapter 5 Managing Application Users > Managing User Accounts: Procedure, Managing User Roles**.

The line manager is both a line manager and an employee. Add the new employee and line manager abstract roles to one or more test line manager users.

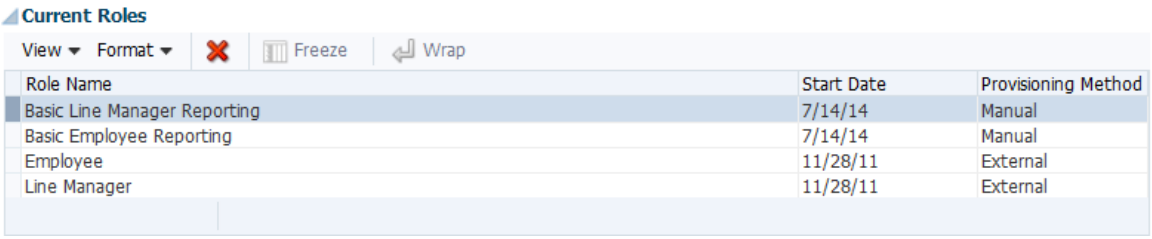


Figure 22. Example of the roles for a user who is a line manager.

Add the new employee abstract role to one or more test employee users.

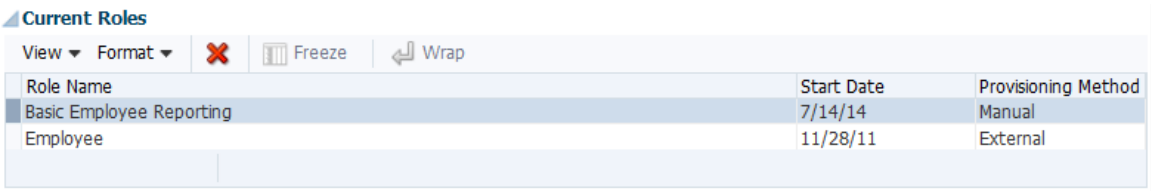


Figure 23. Example of the roles for a user who is an employee.

When testing is complete, return to step 8 and autoprovision provision the roles to all line managers and employees.

Line Managers will be able to see their own data as well as data for workers in their manager hierarchy. For analyses where the line manager should not see their own data, logic will need to be added to exclude their own records. One method is to use the Assignment Manager dimension which is found in every HCM OTBI subject area. The Assignment Manager dimension is secured by manager hierarchy regardless of the security profile in the data role. If you include any attribute from this dimension in the analysis (you can hide it), the results will be limited to data for workers in the manager hierarchy of the user viewing the analysis.

Step 10 Grant Ability to Administer BI and Create BI Publisher Data Models

Sign in with the IT Security Manager job role and follow these steps:

1. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.
2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

The Oracle Entitlements Server Authorization Management page opens.

3. On the Home tab, in the Application Name section, select **obi**.

   In the **Application Roles** section, click Search.

   The obi Role Catalog page opens.

4. In the search results section, select **BI Administrator Role** and click **Open**.

   The BI Administrator Role page opens.

5. Select the **External User Mapping tab**.
6. Add the users who need the ability to administer BI and create BI Publisher data models.
7. Close the Authorization Management page and sign out.

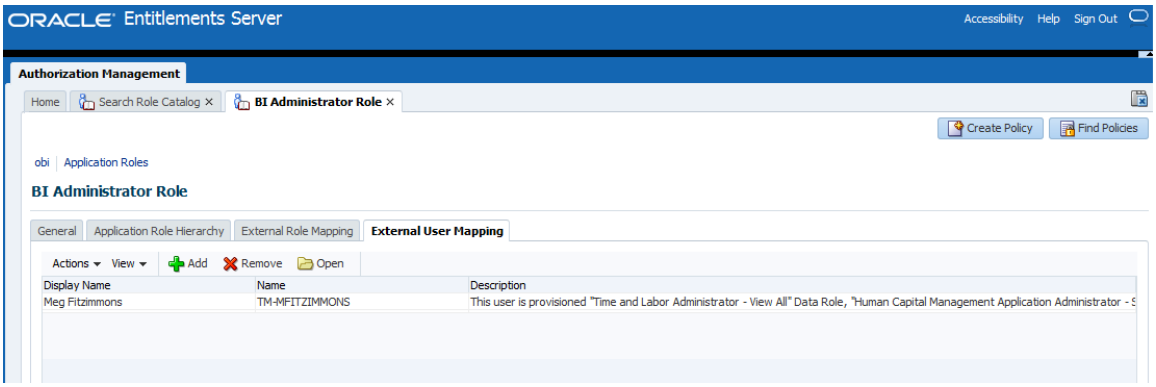


Figure 24. Users specified in External User Mapping tab of the BI Administrator Role.

Testing and Debugging

Create simple sample analyses with a master user, such as a user having a data role with the Human Resource Analyst job role. Save the analysis to a folder within the Shared / Custom folder path. Do not apply any filters.

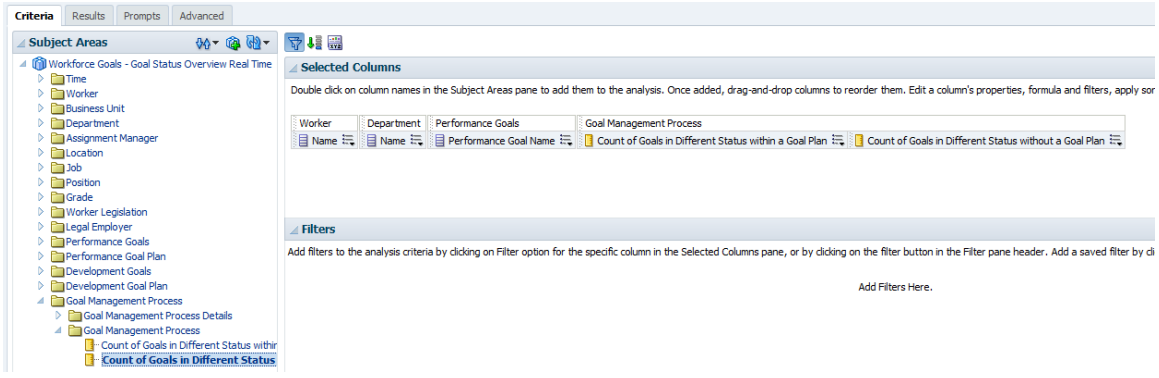


Figure 25. Example of a simple analysis using the Workforce Goals- Goal Status Overview Real Time subject area.

Click on results to ensure that your master user can see data.

Login as each test user.

- Line managers and employees should not be able to create BI Analysis. The option to create analyis will not be visible (BI Answers) or there will be no OTBI subject areas when selecting subject areas for new analysis (Reporting and Analytics).
- Line Managers should see their own data and the data of workers in their line manager hierarchy.
- Employees should only see their own data.
- Users with the BI Author role role should be able to create analysis.
- Users with the BI Administrator role should be able to create BI Publisher Data models by selecting New Data Model from within BI Answers.

If settings are not taking effect:

- Clear local browser cache.
- Restart BI Server to clear the BI Server Cache. If you don't know how to do this, log an SR.

If your user can create analysis and should not be able to, remove the BI Author role from the duties, job role or abstract role inherited by the user. Ensure that the BI Author role is re-granted to users who need it.

- Check the obi duties in the job or abstract roles assigned to the user.
- Open the BI Author role. Ensure that no roles provsioned to the user are listed in the External Role Mapping tab. Ensure that the user is not listed in the External User Mapping tab.

If there are nulls in all rows for columns where data is expected:

- Check the duties in the job or abstract roles assigned to the user. Make sure that you are not missing hcm Transaction Analysis Duty duties. A common mistake is to forget the hcm Workforce Transaction Analysis Duty which results in null Worker, Dept, Job, etc data.
- Check the security profiles in the abstract role or data roles assigned to the user. Make sure that the security profile that applies to the null data does not have a profile that restricts the user from seeing this data.

If the user doesn't see any results

- Check the user's roles.
    - Ensure that the user has been provisioned an abstract role or data role that inherits both the obi and hcm transaction analysis duties for the subject area.
    - Ensure that the user was not assigned a job role directly, which does not have security policies. A data role is required for a job role.
- Check the security profiles in the data role or abstract role which inherits the obi and hcm transaction analysis duties for the subject area. Ensure that the security profiles allow the user to see the expected data.

If the user is seeing the wrong data:

- Check the security profile in the data role or abstract role which inherits the transaction analysis duties for the subject area.
- Check the logic in the analysis.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Hardware and Software, Engineered to Work Together


Oracle is committed to developing practices and products that help protect the environment