Oracle Human Capital Management Cloud
Securing Oracle HCM Cloud

Release 8

April 2014
# Contents

## 1 An Overview of HCM Security in the Cloud
- Securing Oracle HCM Cloud: Overview .......................................................... 1-1
- Role-Based Security: Explained ................................................................. 1-2
- Predefined HCM Roles: Explained ........................................................... 1-3
- Role Types: Explained .............................................................................. 1-4
- Role Inheritance: Explained .................................................................... 1-5
- Duty Role Components: Explained .......................................................... 1-7
- Security Customization: Points to Consider ............................................. 1-8
- Reviewing Predefined Roles in the Security Reference Manuals: Explained .................................................. 1-8

## 2 Implementation Users
- Implementation Users: Explained ......................................................... 2-1
- Creating Implementation Users ............................................................... 2-2
- Creating HCM Data Roles for Implementation Users ............................... 2-9
- Enabling Basic Data Access for Abstract Roles ....................................... 2-18
- Assigning Abstract and Data Roles to HCMUser Implementation User ................................. 2-21
- Resetting the Service Administrator Sign-In Details: Procedure ................. 2-25

## 3 Preparing for Application Users
- Preparing for Application Users: Overview ............................................. 3-1
- User and Role-Provisioning Setup: Critical Choices ................................ 3-1
- User Account Creation Option: Explained ............................................. 3-3
- Default User Name Format Option: Explained ....................................... 3-4
- User Account Role Provisioning Option: Explained ................................ 3-5
- User Account Maintenance Option: Explained ...................................... 3-5
- Send User Name and Password Option: Explained .................................. 3-7
- Setting the User and Role Provisioning Options: Procedure ...................... 3-8
- Oracle Human Capital Management Cloud Password Policy: Explained .... 3-9
- Provisioning Abstract Roles to Users Automatically: Procedure .............. 3-9
- FAQs for Preparing for Application Users .............................................. 3-11

## 4 Creating Application Users
- Creating Application Users: Points to Consider .................................... 4-1
- Creating Oracle HCM Cloud Users Using the New Person Tasks: Procedure ........................................ 4-2
- Creating Oracle HCM Cloud Users Using the Create User Task: Procedure ..................................... 4-3
- FAQs for Creating Application Users ...................................................... 4-5

## 5 Managing Application Users
Managing User Accounts: Procedure ................................................................. 5-1
Changing User Names: Explained ................................................................. 5-3
Sending Personal Data to LDAP: Explained ................................................. 5-3
Processing a User Account Request: Explained ............................................ 5-5
Suspending User Accounts: Explained ....................................................... 5-5
FAQs for Managing Application Users ....................................................... 5-6

6 Provisioning Roles to Application Users
Role Mappings: Explained ....................................................................... 6-1
Creating a Role Mapping: Procedure ....................................................... 6-3
Role Mappings: Examples ....................................................................... 6-4
Role Provisioning and Deprovisioning: Explained ..................................... 6-6
Applying Autoproservation: Explained ...................................................... 6-7
Role Status Values: Explained ............................................................... 6-8
Role Provisioning Status Values: Explained ............................................. 6-9
FAQs for Provisioning Roles to Application Users ..................................... 6-10

7 Creating HCM Data Roles
HCM Data Roles and Security Profiles ..................................................... 7-1
Person Security Profiles .......................................................................... 7-11
Organization and Other Security Profiles ............................................... 7-20
Managing HCM Data Roles ................................................................. 7-27

8 HCM Security in OIM and APM
Security Terminology: Explained ............................................................ 8-1
Reviewing Roles and Role Assignments in Oracle Identity Manager: Procedure 8-2
Reviewing the Duties of a Predefined Job Role: Procedure ..................... 8-3

9 Customizing Security
Creating Custom Job or Abstract Roles ..................................................... 9-1
Creating Custom DutyRoles .................................................................... 9-4
Regenerating HCM Data Roles: Procedure ............................................. 9-8
Enabling Access to HCM Audit Data: Points to Consider ......................... 9-9

10 Synchronizing User and Role Information with Oracle Identity Management
Synchronization of User and Role Information with Oracle Identity Management: How It's Processed ................................................................. 10-1
Scheduling the LDAP Daily Processes: Procedure .................................... 10-2
Send Pending LDAP Requests: Explained ............................................. 10-3
Retrieve Latest LDAP Changes: Explained ........................................... 10-4

11 Specialized Security
Preface

This Preface introduces the guides, online help, and other information sources available to help you more effectively use Oracle Fusion Applications.

Oracle Fusion Applications Help

You can access Oracle Fusion Applications Help for the current page, section, activity, or task by clicking the help icon. The following figure depicts the help icon.

Note

If you don’t see any help icons on your page, then click the Show Help icon button in the global area. However, not all pages have help icons.

You can add custom help files to replace or supplement the provided content. Each release update includes new help content to ensure you have access to the latest information. Patching does not affect your custom help content.

Oracle Fusion Applications Guides

Oracle Fusion Applications guides are a structured collection of the help topics, examples, and FAQs from the help system packaged for easy download and offline reference, and sequenced to facilitate learning. To access the guides, go to any page in Oracle Fusion Applications Help and select Documentation Library from the Navigator menu.

Guides are designed for specific audiences:

- **User Guides** address the tasks in one or more business processes. They are intended for users who perform these tasks, and managers looking for an overview of the business processes. They are organized by the business process activities and tasks.

- **Implementation Guides** address the tasks required to set up an offering, or selected features of an offering. They are intended for implementors. They are organized to follow the task list sequence of the offerings, as displayed within the Setup and Maintenance work area provided by Oracle Fusion Functional Setup Manager.

- **Concept Guides** explain the key concepts and decisions for a specific area of functionality. They are intended for decision makers, such as chief
financial officers, financial analysts, and implementation consultants. They are organized by the logical flow of features and functions.

- **Security Reference Manuals** describe the predefined data that is included in the security reference implementation for one offering. They are intended for implementors, security administrators, and auditors. They are organized by role.

These guides cover specific business processes and offerings. Common areas are addressed in the guides listed in the following table.

<table>
<thead>
<tr>
<th>Guide</th>
<th>Intended Audience</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common User Guide</td>
<td>All users</td>
<td>Explains tasks performed by most users.</td>
</tr>
<tr>
<td>Common Implementation Guide</td>
<td>Implementors</td>
<td>Explains tasks within the Define Common Applications Configuration task list, which is included in all offerings.</td>
</tr>
<tr>
<td>Functional Setup Manager User Guide</td>
<td>Implementors</td>
<td>Explains how to use Oracle Fusion Functional Setup Manager to plan, manage, and track your implementation projects, migrate setup data, and validate implementations.</td>
</tr>
<tr>
<td>Technical Guides</td>
<td>System administrators, application developers, and technical members of implementation teams</td>
<td>Explain how to install, patch, administer, and customize Oracle Fusion Applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Limited content applicable to Oracle Cloud implementations.</td>
</tr>
</tbody>
</table>

For other guides, go to Oracle Technology Network at http://www.oracle.com/technetwork/indexes/documentation.

**Other Information Sources**

**My Oracle Support**

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.
Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications provides details on service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes.

In Oracle Fusion Applications, you can use Oracle Enterprise Repository at http://fusionappsoer.oracle.com for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.

- Other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww_grp@oracle.com. You can use Send Feedback to Oracle from the Settings and Actions menu in Oracle Fusion Applications Help.
Securing Oracle HCM Cloud: Overview

Oracle Human Capital Management Cloud is secure as delivered. This guide explains how to enable user access to HCM functions and data. You perform many of the tasks in this guide during implementation. You can also perform most of them later and as requirements change. This topic summarizes the scope of this guide and identifies the contents of each chapter.

Guide Structure

This table describes the contents of each chapter in this guide.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Overview of HCM Security in the Cloud</td>
<td>A brief introduction to the concepts of role-based security</td>
</tr>
<tr>
<td>Implementation Users</td>
<td>The role of implementation users and instructions for creating them</td>
</tr>
<tr>
<td>Preparing for Application Users</td>
<td>Enterprise-wide options and related decisions that affect application users</td>
</tr>
<tr>
<td>Creating Application Users</td>
<td>The ways in which you can create application users, with instructions for some methods</td>
</tr>
<tr>
<td>Managing Application Users</td>
<td>How to maintain user accounts throughout the workforce lifecycle</td>
</tr>
<tr>
<td>Provisioning Roles to Application Users</td>
<td>The ways in which application users can acquire roles, with instructions for creating some standard role mappings</td>
</tr>
<tr>
<td>Creating HCM Data Roles</td>
<td>How to create HCM data roles and use HCM security profiles to identify the data that users can access</td>
</tr>
</tbody>
</table>
During implementation, you can perform security-related tasks:

- From an implementation project
- By opening the Setup and Maintenance work area

Select **Navigator - Tools - Setup and Maintenance** and search for the task on the All Tasks tab.

Once the implementation is complete, you can perform most security-related tasks from the Setup and Maintenance work area. Any exceptions are identified in relevant topics. For example, you hire workers in the New Person work area, not the Setup and Maintenance work area.

**Role-Based Security: Explained**

In Oracle Fusion Applications, users have roles through which they gain access to functions and data. Users can have any number of roles.

In this figure, user Linda Swift has three roles.

When Linda signs in to Oracle Fusion Human Capital Management (Oracle Fusion HCM), she doesn't have to select a role. All of these roles are active concurrently.
The functions and data that Linda can access are determined by this combination of roles.

- As an employee, Linda can access employee functions and data.
- As a line manager, Linda can access line-manager functions and data.
- As a human resource specialist (HR specialist), Linda can access HR specialist functions and data for Vision Operations.

**Role-Based Access Control**

Role-based security in Oracle Fusion Applications controls who can do what on which data.

In role-based access:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who</td>
<td>Is a role assigned to a user</td>
</tr>
<tr>
<td>What</td>
<td>Is a function that users with the role can perform</td>
</tr>
<tr>
<td>Which Data</td>
<td>Is the set of data that users with the role can access when performing the function</td>
</tr>
</tbody>
</table>

For example:

<table>
<thead>
<tr>
<th>Who</th>
<th>What</th>
<th>Which Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line managers</td>
<td>Can create performance documents</td>
<td>For workers in their reporting hierarchies</td>
</tr>
<tr>
<td>Employees</td>
<td>Can view payslips</td>
<td>For themselves</td>
</tr>
<tr>
<td>Payroll managers</td>
<td>Can report payroll balances</td>
<td>For specified payrolls</td>
</tr>
<tr>
<td>HR specialists</td>
<td>Can transfer workers</td>
<td>For workers in specified organizations</td>
</tr>
</tbody>
</table>

**Predefined HCM Roles: Explained**

Many job and abstract roles are predefined in Oracle Fusion Human Capital Management (Oracle Fusion HCM). This list shows the main predefined HCM roles:

- Benefits Administrator
- Benefits Manager
- Benefits Specialist
- Compensation Administrator
• Compensation Analyst
• Compensation Manager
• Compensation Specialist
• Contingent Worker
• Employee
• Human Capital Management Application Administrator
• Human Resource Analyst
• Human Resource Manager
• Human Resource Specialist
• Human Resource VP
• Line Manager
• Payroll Administrator
• Payroll Manager

These predefined roles are part of the Oracle Fusion HCM Security Reference Implementation. The Security Reference Implementation is a predefined set of security definitions that you can use as supplied.

Also included in the Security Reference Implementation are roles that are common to all Oracle Fusion applications, such as:

• Application Implementation Consultant
• IT Security Manager

You can include the predefined roles in HCM data roles, for example. Typically, you assign the Employee, Contingent Worker, and Line Manager abstract roles directly to users.

Role Types: Explained

Oracle Fusion Human Capital Management (Oracle Fusion HCM) defines four types of roles:

• Data roles
• Abstract roles
• Job roles
• Duty roles

This topic introduces the role types.

Data Roles

Data roles combine a worker’s job and the data that users with the job must access. For example, the HCM data role Payroll Administrator Payroll US combines a job (Payroll Administrator) with a data scope (Payroll US). You define the data scope of a data role in one or more HCM security profiles.
HCM data roles aren't part of the security reference implementation. You define all HCM data roles locally and assign them directly to users.

Abstract Roles

Abstract roles represent a worker’s role in the enterprise independently of the job that you hire the worker to do. Three abstract roles are predefined in Oracle Fusion HCM:

- Employee
- Contingent worker
- Line manager

You can also create custom abstract roles. All workers are likely to have at least one abstract role through which they access standard functions, such as managing their own information and searching the worker directory.

You assign abstract roles directly to users.

Job Roles

Job roles represent the job that you hire a worker to perform. Human Resource Analyst and Payroll Manager are examples of predefined job roles. You can also create custom job roles.

Typically, you include job roles in data roles and assign those data roles to users. The IT Security Manager and Application Implementation Consultant predefined job roles are exceptions to this general rule because they’re not considered HCM job roles. Also, you don’t define their data scope in HCM security profiles.

Duty Roles

Duty roles represent the individual duties that users perform as part of their job. They grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on. Job roles and abstract roles inherit duty roles. Duty roles can also inherit other duty roles. They’re part of the security reference implementation, and are the building blocks of custom job and abstract roles.

You don’t assign duty roles directly to users.

Role Inheritance: Explained

Each role is a hierarchy of other roles:

- HCM data roles inherit job or abstract roles.
- Job and abstract roles inherit duty roles.
- Duty roles can inherit other duty roles.

In addition, when you assign data and abstract roles to users, they inherit the data and function security associated with those roles.
Role Inheritance Example

This example shows how roles are inherited.

The figure shows a few representative duty roles. In reality, job and abstract roles inherit many duty roles, which themselves may inherit many duty roles.

In this example, user Tom Green has two roles:
- HR Specialist Vision Corporation, a data role
- Employee, an abstract role

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| HR Specialist Vision Corporation    | Inherits the job role Human Resource Specialist. In turn, this job role inherits the duty roles that provide access to the tasks and functions that a human resource specialist performs.  
                                         The security profile assigned to the data role provides the data access for the role. |
| Employee                            | Inherits the duty roles that provide access to all tasks and functions, unrelated to a specific job, that every employee performs.     
                                         The security profile assigned to the abstract role provides the data access for the role. |
**Duty Role Components: Explained**

Duty roles are associated with function security privileges and data security policies.

For example, the Worker Promotion Duty is associated with one function security privilege and two data security policies.

- The function security privilege Promote Worker secures access to the Promote Worker page.
- The data security policy Promote Worker Data determines the workers whom users with this duty role can promote.
- The data security policy Choose Position Data determines the positions into which users with this duty role can promote workers.

**Data Security Policies**

Each data security policy combines:

- A duty role.
  For example, Worker Promotion Duty.
- A business object being accessed.
  For example, Person Assignment.
- The condition that must be met for access to be granted.
  For example, human resource specialists can promote workers whose person and assignment records are identified in their person and assignment security profiles.
- A data security privilege that defines the action being performed.
  For example, Promote Worker.

**Function Security Privileges**

Each function security privilege secures the code resources that make up the relevant page, such as the Promote Worker page.
Security Customization: Points to Consider

If the predefined security reference implementation doesn’t fully represent your enterprise, then you can make changes.

For example, the predefined Line Manager abstract role includes compensation management duties. If some of your line managers don’t handle compensation, then you can create a custom line manager role without those duties. Alternatively, if a predefined job role is too narrowly defined, then you can create a job role with a greater range of duties than its predefined equivalent.

During your implementation of Oracle Fusion Human Capital Management, you evaluate the predefined roles and decide whether changes are needed.

Tip

If you change the security reference implementation, then the recommendation is to create custom roles rather than modify predefined roles. Upgrade and maintenance patches to the security reference implementation preserve your changes. Therefore, if you modify predefined roles, you can’t restore them to their original state by upgrading.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren’t represented in the security reference implementation, then you create a job or abstract role.

Predefined Roles with Different Duties

If the duties for a predefined job role don’t match the corresponding job in your enterprise, then you add duties to or subtract duties from the job role.

Predefined Roles with Missing Duties

If the duties for a job aren’t defined in the security reference implementation, then you create custom duty roles.

Reviewing Predefined Roles in the Security Reference Manuals: Explained

The Security Reference for Oracle HCM Cloud includes descriptions of all predefined security data in the Oracle Fusion Human Capital Management security reference implementation. The Security Reference for Oracle
Applications Cloud includes descriptions of all predefined security data that's common to Oracle Fusion Applications.

You can access all information in these manuals from various Oracle Fusion HCM user interface pages. For example, you can review individual job roles using the Manage Job Roles task. However, using the manuals you can compare roles and plan any changes.

You can access the security reference manuals on cloud.oracle.com. Select Resources - Getting Started - Documentation - All Books.

**Security Reference for Oracle HCM Cloud**

The Security Reference for Oracle HCM Cloud contains a section for each predefined HCM job and abstract role. For each role, you can review its:

- Duties
- Role hierarchy
- Function security privileges
- Data security policies

This information can help you to identify which users need each role and whether to make any changes before provisioning roles.
Implementation Users: Explained

Implementation users:

- Manage implementation projects for Oracle Human Capital Management Cloud (Oracle HCM Cloud).
- Administer Oracle HCM Cloud users and security, both during and after implementation.
- Set up basic enterprise structures for an Oracle HCM Cloud service.

Implementation users have the necessary access for both initial implementation of the Oracle HCM Cloud service and its ongoing maintenance. You're recommended to create at least one implementation user.

How Implementation Users Differ from Application Users

Thanks to job roles such as Application Implementation Consultant, implementation users have unrestricted access to large amounts of data. However, the need for this level of access is temporary. After implementation, both application users and administrators can perform their tasks using less powerful roles.

For an implementation user, only a user account exists. No person record exists in Oracle Fusion Human Capital Management (Oracle Fusion HCM).

Who Creates Implementation Users?

The Oracle HCM Cloud service administrator creates initial implementation users.

Recommended Implementation Users

You're recommended to create the following implementation users to ensure segregation of critical duties:

<table>
<thead>
<tr>
<th>Implementation User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIMAdmin</td>
<td>Accesses Oracle Identity Management (OIM) through the Oracle HCM Cloud service. This user is intended for security administrators.</td>
</tr>
<tr>
<td>Implementation User</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TechAdmin</td>
<td>Performs technical setup duties, including security setup. This user is intended for technical super users.</td>
</tr>
<tr>
<td>HCMUser</td>
<td>Performs functional setup duties. This user is intended for users who are performing the Oracle HCM Cloud implementation steps.</td>
</tr>
</tbody>
</table>

Additional implementation users may be useful, depending on the size of the enterprise and the structure of the implementation team. For example:

- An implementation project manager can assign implementation tasks to other implementation users. This implementation user has the Application Implementation Manager job role.
- A product family application administrator can perform implementation tasks for a specific product. This approach may be of interest if you're implementing multiple Oracle Fusion products and want an implementor for each product.

The Human Capital Management Application Administrator job role can access only HCM setup tasks. The Application Implementation Consultant job role can access all Oracle Fusion Applications setup tasks.

Creating Implementation Users

Creating Implementation Users: Overview

As the service administrator for the Oracle HCM Cloud service, you're sent sign-in details when your environments are provisioned. This topic summarizes how to access the service for the first time and set up implementation users to perform the implementation. You must complete these steps before you release the environment to your implementation team.

Tip
Create implementation users in the test environment first. Migrate your implementation to the production environment only after you have validated it. With this approach, the implementation team can learn how to implement security before setting up application users in the production environment.

Signing In to the Oracle HCM Cloud Service

The service activation mail from Oracle provides the service URLs, user name, and temporary password for the test or production environment. Refer to the email for the environment that you’re setting up. The Identity Domain value is the environment name. For example, HCMA could be the production environment and HCMA-TEST could be the test environment.

Sign in to the test or production Oracle HCM Cloud service using the service home URL from the service activation mail. The URL ends with either AtkHomePageWelcome or HcmFusionHome.
When you first sign in, use the password in the service activation mail. You’re prompted to change the password and answer some challenge questions. Make a note of the new password, which is the service administrator password for subsequent access to the service.

You’re recommended not to share your sign-in details with other users.

**Creating Implementation Users**

This table summarizes the process of creating implementation users and assigning roles to them.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task or Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create Implementation Users</td>
<td>You create the implementation users OIMAdmin, TechAdmin, and HCMUser and assign the required job roles to them if these users don’t already exist in your environment. You don’t associate named workers with these users at this time because your Oracle HCM Cloud service isn’t yet configured to onboard workers. As your implementation progresses, you may decide to replace these users or change their definitions. However, these three are required initially.</td>
</tr>
<tr>
<td>2</td>
<td>Run User and Roles Synchronization Process</td>
<td>You run the process Retrieve Latest LDAP Changes to copy changes made in Oracle Identity Management (OIM) to Oracle Fusion Human Capital Management (Oracle Fusion HCM).</td>
</tr>
</tbody>
</table>
| 3    | Create Data Roles for Implementation Users | To enable implementation users to access HCM data, you create the following data roles: 
HRAnalyst_ViewAll 
HCMAplicationAdministrator_ViewAll 
HR_Specialist_ViewAll
You create additional data roles if you have licensed the Oracle Fusion Workforce Compensation Cloud Service, the Oracle Fusion Global Payroll Cloud Service, or the Oracle Fusion Global Payroll Interface Cloud Service. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Task or Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Assign Security Profiles to Abstract Roles</td>
<td>Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles.</td>
</tr>
<tr>
<td>5</td>
<td>Create a Generic Role Mapping for HCM Data Roles</td>
<td>Enable the HCM data roles created in step 3 to be provisioned to implementation users.</td>
</tr>
<tr>
<td>6</td>
<td>Assign Abstract and Data Roles to the HCMUser Implementation User</td>
<td>Assign roles to the HCMUser implementation user that enable functional implementation to proceed.</td>
</tr>
<tr>
<td>7</td>
<td>Verify HCMUser Access</td>
<td>Confirm that the HCMUser implementation user can access the functions enabled by the assigned roles.</td>
</tr>
</tbody>
</table>

Once these steps are complete, you’re recommended to reset the service administrator sign-in details.

Creating the OIMAdmin Implementation User : Procedure

This topic describes how to create the OIMAdmin implementation user and assign roles to the user.

Creating the OIMAdmin Implementation User

Sign in as the Oracle HCM Cloud service administrator 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 task Create Implementation Users.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click **Administration** in the top-right of the page.
4. In the Users section of the Welcome tab on the Delegated Administration page, click **Create User**.

Complete the fields on the Create User page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>OIMAdmin</td>
</tr>
<tr>
<td>Display Name</td>
<td>OIMAdmin</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
</tr>
<tr>
<td>User Type</td>
<td>Non Worker</td>
</tr>
<tr>
<td>User Login</td>
<td>OIMAdmin</td>
</tr>
<tr>
<td>Password</td>
<td>Any value that complies with the password policy</td>
</tr>
</tbody>
</table>

To view the password policy, click the Help icon by the Password field.

**Note**

Make a note of the password. The user who first signs in as OIMAdmin must change the password.

5. Click **Save**.
   A series of tabs appears on the Create User page.

**Assigning Roles to OIMAdmin**

To assign the IT Security Manager job role to the OIMAdmin implementation user, follow these steps:

1. On the Create User page, click the Roles tab.
2. On the Roles tab, click **Assign**.
3. Search for and select the IT Security Manager job role.
   The IT Security Manager job role now appears on the Roles tab.
4. Click **Close Single Tab** to close the Create User page and return to the Oracle Identity Manager - Delegated Administration page.

**Creating the TechAdmin Implementation User:** Procedure

This topic describes how to create the TechAdmin implementation user and assign roles to the user.

**Creating the TechAdmin Implementation User**

If you have just created the OIMAdmin implementation user and are on the Oracle Identity Manager - Delegated Administration page, then follow this procedure from step 4. Otherwise, sign in as the Oracle HCM Cloud service administrator 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 task Create Implementation Users.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click **Administration** in the top-right of the page.

4. In the Users section of the Welcome tab on the Oracle Identity Manager - Delegated Administration page, click **Create User**.

   Complete the fields on the Create User page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>TechAdmin</td>
</tr>
<tr>
<td>Display Name</td>
<td>TechAdmin</td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
</tr>
<tr>
<td>User Type</td>
<td>Non Worker</td>
</tr>
<tr>
<td>User Login</td>
<td>TechAdmin</td>
</tr>
<tr>
<td>Password</td>
<td>Any value that complies with the password policy</td>
</tr>
</tbody>
</table>

To view the password policy, click the **Help** icon by the **Password** field.

**Note**

Make a note of the password. The user who first signs in as TechAdmin must change the password.

5. Click **Save**.

   A series of tabs appears on the Create User page.

**Assigning Roles to TechAdmin**

To assign job roles to the TechAdmin implementation user, follow these steps:

1. On the Create User page, click the Roles tab.
2. On the Roles tab, click **Assign**.
3. Search for and select the following job roles:
   - IT Security Manager
   - Application Implementation Consultant
   - Administrators: Weblogic access
   - Application Diagnostics Administrator
   - Application Diagnostics Advanced User
These five job roles now appear on the Roles tab.

4. Click **Close Single Tab** to close the Create User page and return to the Oracle Identity Manager - Delegated Administration page.

---

**Important**

Application Implementation Consultant is a powerful role that has unrestricted access to a large amount of data. Once the implementation is complete, you’re recommended to revoke this role from all users using the Revoke Data Role from Implementation Users task. For ongoing maintenance of Oracle HCM Cloud setup data, use a less powerful role, such as an HCM data role based on the Human Capital Management Application Administrator role.

---

**Creating the HCMUser Implementation User : Procedure**

This topic explains how to create the HCMUser implementation user and assign roles to the user.

**Creating the HCMUser Implementation User**

If you have just created the OIMAdmin or TechAdmin implementation user and are on the Oracle Identity Manager - Delegated Administration page, then follow this procedure from step 4. Otherwise, sign in as the Oracle HCM Cloud service administrator 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 task Create Implementation Users.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click **Administration** in the top-right of the page.
4. In the Users section of the Welcome tab on the Oracle Identity Manager - Delegated Administration page, click **Create User**.

Complete the fields on the Create User page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>HCMUser</td>
</tr>
<tr>
<td>Display Name</td>
<td>HCMUser</td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
</tr>
<tr>
<td>User Type</td>
<td>Non Worker</td>
</tr>
<tr>
<td>User Login</td>
<td>HCMUser</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Any value that complies with the password policy</td>
</tr>
</tbody>
</table>

To view the password policy, click the **Help** icon by the **Password** field.

**Note**

Make a note of the password. The user who first signs in as HCMUser must change the password.

5. Click **Save**.
   
   A series of tabs appears on the Create User page.

**Assigning Roles to HCMUser**

To assign job roles to the HCMUser implementation user, follow these steps:

1. On the Create User page, click the Roles tab.
2. On the Roles tab, click **Assign**.
3. Search for and select the following job roles:
   - Application Administrator
   - Application Implementation Consultant
   - Application Diagnostics Regular User
   - Application Diagnostics Viewer
   
   These four job roles now appear on the Roles tab.
4. Click **Close Single Tab** to close the Create User page and return to the Oracle Identity Manager - Delegated Administration page.

Close the Oracle Identity Manager Delegated Administration Console tab.

**Important**

Application Implementation Consultant is a powerful role that has unrestricted access to a large amount of data. Once the implementation is complete, you’re recommended to revoke this role from all users using the Revoke Data Role from Implementation Users task. For ongoing maintenance of Oracle HCM Cloud setup data, use a less powerful role, such as an HCM data role based on the Human Capital Management Application Administrator role.

**Synchronizing User and Role Information: Procedure**

You run the process Retrieve Latest LDAP Changes during implementation whenever you make changes directly in Oracle Identity Management (OIM).

This process copies your changes to Oracle Fusion Human Capital Management
(Oracle Fusion HCM). To run this process, perform the task Run User and Roles Synchronization Process as described in this topic.

**Running the Retrieve Latest LDAP Changes Process**

1. Sign in to the Oracle HCM Cloud service environment as the TechAdmin user.
   
   If this is the first use of this user name, then you’re prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the password, the challenge questions, and their answers. You use the updated password whenever you sign in as this user subsequently.

2. Select **Navigator - Tools - Setup and Maintenance** to open the Setup and Maintenance work area.

3. On the All Tasks tab of the Overview page, search for and select the task Run User and Roles Synchronization Process.
   
   The process submission page for the Retrieve Latest LDAP Changes process opens.

4. Click **Submit**.

5. Click **OK** to close the confirmation message.

**Important**

During implementation, whenever you make changes to user and role information directly in OIM, you must run the Retrieve Latest LDAP Changes process as described here. Otherwise, the changes you make in OIM don’t appear in Oracle Fusion HCM.

**Creating HCM Data Roles for Implementation Users**

Creating HCM Data Roles for Implementation Users: Explained

You create HCM data roles to enable the HCMUser implementation user to access HCM data and complete the functional implementation. This topic introduces the HCM data roles that you must create.

Create the following HCM data roles:

- HRAnalyst_ViewAll
- HCMApplicationAdministrator_ViewAll
- HRSpecialist_ViewAll

If you have licensed the Oracle Fusion Workforce Compensation Cloud Service, then you need also to create the following HCM data roles:

- CompensationAdmin_ViewAll
- CompensationMgr_ViewAll

If you have licensed the Oracle Fusion Global Payroll Cloud Service or the Oracle Fusion Global Payroll Interface Cloud Service, then you need also to create the following HCM data roles:

- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll
Creating the HRAnalyst_ViewAll Data Role: Procedure

This topic describes how to create the HRAnalyst_ViewAll data role. This role is one of several that the HCMUser implementation user must have to complete the functional implementation.

Creating the HRAnalyst_ViewAll Data Role

Sign in to the Oracle HCM Cloud service as the TechAdmin user, 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 task Manage Data Role and Security Profiles.

3. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.

4. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>HRAnalyst_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Human Resource Analyst</td>
</tr>
</tbody>
</table>

5. Click **Next**.

6. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Public Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Document Type</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll Flow</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>
7. Click Review.

8. On the Create Data Role: Review page, click Submit.

9. On the Manage Data Role and Security Profiles page, search for the role HRAnalyst_ViewAll. The role status is Complete when the role exists in both Oracle Identity Management and Oracle Fusion Human Capital Management.

Creating the HCMApplicationAdministrator_ViewAll Data Role: Procedure

This topic describes how to create the HCMApplicationAdministrator_ViewAll data role. This role is one of several that the HCMUser implementation user must have to complete the functional implementation.

Creating the HCMApplicationAdministrator_ViewAll Data Role

If you have just created a different implementation data role and are on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in to the Oracle HCM Cloud service as the TechAdmin user 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 task Manage Data Role and Security Profiles.

3. In the Search Results section of the Manage Data Roles and Security Profiles page, click Create.

4. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>HCMApplicationAdministrator_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Human Capital Management Application Admin</td>
</tr>
</tbody>
</table>

5. Click Next.

6. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles:

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Countries</td>
<td>View All Countries</td>
</tr>
</tbody>
</table>
Creating the HRSpecialist_ViewAll Data Role: Procedure

This topic describes how to create the HRSpecialist_ViewAll data role. This role is one of several that the HCMUser implementation user must have to complete the functional implementation.

**Creating the HRSpecialist_ViewAll Data Role**

If you have just created a different implementation data role and are on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in to the Oracle HCM Cloud service as the TechAdmin user 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 task Manage Data Role and Security Profiles.

3. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.

4. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>HRSpecialist_ViewAll</td>
</tr>
</tbody>
</table>

7. Click **Review**.

8. On the Create Data Role: Review page, click **Submit**.

9. On the Manage Data Role and Security Profiles page, search for the role HCMAplicationAdministrator_ViewAll. The role status is Complete when the role exists in both Oracle Identity Management and Oracle Fusion Human Capital Management.
5. Click Next.

6. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Role</td>
<td>Human Resource Specialist</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Countries</td>
<td>View All Countries</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Public Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Document Type</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll</td>
<td>View All Payrolls</td>
</tr>
<tr>
<td>Payroll Flow</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

7. Click Review.

8. On the Create Data Role: Review page, click Submit.

9. On the Manage Data Role and Security Profiles page, search for the role HRSpecialist_ViewAll. The role status is Complete when the role exists in both Oracle Identity Management and Oracle Fusion Human Capital Management.

Creating HCM Data Roles for Oracle Fusion Workforce Compensation
Implementation Users: Procedure

If you have licensed the Oracle Fusion Workforce Compensation Cloud Service, then you create the following HCM data roles:

- CompensationAdmin_ViewAll
- CompensationMgr_ViewAll

This topic explains how to create these roles by performing the Manage Data Role and Security Profiles task.
Creating the CompensationAdmin_ViewAll Data Role

If you have just created a different implementation data role and are on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in to the Oracle HCM Cloud service as the TechAdmin user 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 task Manage Data Role and Security Profiles.

3. In the Search Results section of the Manage Data Roles and Security Profiles page, click Create.

4. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>CompensationAdmin_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Compensation Administrator</td>
</tr>
</tbody>
</table>

5. Click Next.

6. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Public Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Document Type</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll</td>
<td>View All Payrolls</td>
</tr>
<tr>
<td>Payroll Flow</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

7. Click Review.

8. On the Create Data Role: Review page, click Submit.
9. On the Manage Data Role and Security Profiles page, search for the role CompensationAdmin_ViewAll. The role status is Complete when the role exists in both Oracle Identity Management (OIM) and Oracle Fusion Human Capital Management (Oracle Fusion HCM).

**Creating the CompensationMgr_ViewAll Data Role**

Follow these steps:

1. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
2. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>CompensationMgr_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Compensation Manager</td>
</tr>
</tbody>
</table>

3. Click **Next**.
4. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Countries</td>
<td>View All Countries</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Public Person</td>
<td>View All People</td>
</tr>
<tr>
<td>Document Type</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll Flow</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

5. Click **Review**.
6. On the Create Data Role: Review page, click **Submit**.
7. On the Manage Data Role and Security Profiles page, search for the role CompensationMgr_ViewAll. The role status is Complete when the role exists in both OIM and Oracle Fusion HCM.
Creating HCM Data Roles for Oracle Fusion Global Payroll Implementation

Users: Procedure

If you have licensed the Oracle Fusion Global Payroll Cloud Service or the Oracle Fusion Global Payroll Interface Cloud Service, then you create the following HCM data roles:

- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll

This topic explains how to create these roles using the Manage Data Role and Security Profiles task.

Creating the PayrollAdmin_ViewAll Data Role

If you have just created a different implementation data role and are on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in to the Oracle HCM Cloud service as the TechAdmin user 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 in the Setup and Maintenance work area, search for and select the task Manage Data Role and Security Profiles.

3. In the Search Results section of the Manage Data Roles and Security Profiles page, click Create.

4. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>PayrollAdmin_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Payroll Administrator</td>
</tr>
</tbody>
</table>

5. Click Next.

6. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
</tbody>
</table>
Creating the PayrollMgr_ViewAll Data Role

Follow these steps:

1. In the Search Results section of the Manage Data Roles and Security Profiles page, click Create.

2. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role Name</td>
<td>PayrollMgr_ViewAll</td>
</tr>
<tr>
<td>Job Role</td>
<td>Payroll Manager</td>
</tr>
</tbody>
</table>

3. Click Next.

4. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles.

<table>
<thead>
<tr>
<th>Section</th>
<th>Security Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Legislative Data Group</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person</td>
<td>View All People</td>
</tr>
</tbody>
</table>
5. Click **Review**.

6. On the Create Data Role: Review page, click **Submit**.

7. On the Manage Data Role and Security Profiles page, search for the role `PayrollMgr_ViewAll`. The role status is Complete when the role exists in both OIM and Oracle Fusion HCM.

### Enabling Basic Data Access for Abstract Roles

#### Assigning Security Profiles to Abstract Roles: Explained

These abstract roles are predefined in Oracle Fusion Human Capital Management:

- Employee
- Contingent worker
- Line manager

Users with these roles can sign in to Oracle Fusion Applications and open application pages. However, they have no automatic access to data. For example, employees can open the person gallery but can't view portraits. Line managers can open the Manager Resources Dashboard but can't see data for their organizations.

To enable basic HCM data access for users with abstract roles, you assign security profiles directly to those roles.

#### Predefined Security Profiles to Assign to Abstract Roles

This table identifies the predefined security profiles that you can assign directly to the employee, line manager, and contingent worker roles.

<table>
<thead>
<tr>
<th>Security Profile Type</th>
<th>Employee</th>
<th>Contingent Worker</th>
<th>Line Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person</td>
<td>View Own Record</td>
<td>View Own Record</td>
<td>View Manager Hierarchy</td>
</tr>
<tr>
<td>Public person</td>
<td>View All Workers</td>
<td>View All Workers</td>
<td>View All Workers</td>
</tr>
<tr>
<td>Organization</td>
<td>View All Organizations</td>
<td>View All Organizations</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position</td>
<td>View All Positions</td>
<td>View All Positions</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Security Profile Type</td>
<td>Employee</td>
<td>Contingent Worker</td>
<td>Line Manager</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Legislative data group</td>
<td>View All Legislative Data Groups</td>
<td>View All Legislative Data Groups</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Country</td>
<td>View All Countries</td>
<td>View All Countries</td>
<td>View All Countries</td>
</tr>
<tr>
<td>Document type</td>
<td>View All Document Types</td>
<td>View All Document Types</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>View All Payrolls</td>
</tr>
<tr>
<td>Payroll flow</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

After implementation, you may want to change aspects of this data access. For example, you may want to create your own security profiles and assign those directly to abstract roles.

**Caution**

Such changes apply to all users who have the abstract role.

**HCM Data Roles**

Users who have abstract roles are likely to gain additional data access from the HCM data roles that you define for their job roles. For example, you may create an HCM data role for human resource specialists to access the person records of all workers in a legal employer. Such data access is in addition to any access provided by abstract roles.

**Assigning Security Profiles to Abstract Roles: Worked Example**

To enable basic data access for the predefined employee, contingent worker, and line manager abstract roles, you assign predefined security profiles to them during implementation. This example shows how to assign security profiles to abstract roles using the Manage Data Role and Security Profiles task.

**Searching for the Employee Abstract Role**

1. Sign in to the Oracle HCM Cloud service as the TechAdmin user. On-premises users must sign in with a role that has the IT Security Manager job role.
2. Select **Navigator - Tools - Setup and Maintenance** to open the Setup and Maintenance work area.
3. On the All Tasks tab of the Overview page, search for and select the task **Manage Data Role and Security Profiles**.
4. On the Manage Data Roles and Security Profiles page, enter Employee in the **Role** field. Click **Search**.
5. In the Search Results region, select the predefined Employee role and click **Edit**. The Edit Data Role: Role Details page opens.
Assigning Security Profiles to the Employee Abstract Role

1. On the Edit Data Role: Role Details page, click Next.

2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table. You may see a subset of these security profiles, depending on the combination of cloud services or product offerings that you’re implementing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Security Profile</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position Security Profile</td>
<td>View All Positions</td>
</tr>
<tr>
<td>Country Security Profile</td>
<td>View All Countries</td>
</tr>
<tr>
<td>LDG Security Profile</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person Security Profile (Person section)</td>
<td>View Own Record</td>
</tr>
<tr>
<td>Person Security Profile (Public Person section)</td>
<td>View All Workers</td>
</tr>
<tr>
<td>Document Type Security Profile</td>
<td>View All Document Types</td>
</tr>
</tbody>
</table>

3. Click Review.

4. On the Edit Data Role: Review page, click Submit.

5. On the Manage Data Roles and Security Profiles page, search again for the predefined Employee role.

6. In the Search Results region, confirm that a green check mark appears in the Security Profiles column for the Employee role.
   The check mark confirms that security profiles are assigned to the role.
   Repeat the steps in Searching for the Employee Abstract Role and Assigning Security Profiles to the Employee Abstract Role for the predefined Contingent Worker role.

Searching for the Line Manager Abstract Role

1. On the Manage Data Roles and Security Profiles page, enter Line Manager in the Role field. Click Search.

2. In the Search Results region, select the predefined Line Manager role and click Edit.
   The Edit Data Role: Role Details page opens.

Assigning Security Profiles to the Line Manager Abstract Role

1. On the Edit Data Role: Role Details page, click Next.
2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table. You may see a subset of these security profiles, depending on the combination of cloud services or product offerings that you’re implementing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Security Profile</td>
<td>View All Organizations</td>
</tr>
<tr>
<td>Position Security Profile</td>
<td>View All Positions</td>
</tr>
<tr>
<td>LDG Security Profile</td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td>Person Security Profile (Person section)</td>
<td>View Manager Hierarchy</td>
</tr>
<tr>
<td>Person Security Profile (Public Person section)</td>
<td>View All Workers</td>
</tr>
<tr>
<td>Document Type Security Profile</td>
<td>View All Document Types</td>
</tr>
<tr>
<td>Payroll</td>
<td>View All Payrolls</td>
</tr>
<tr>
<td>Payroll Flow</td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

3. Click **Review**.

4. On the Edit Data Role: Review page, click **Submit**

5. On the Manage Data Roles and Security Profiles page, search again for the predefined Line Manager role.

6. In the search results, confirm that a green check mark appears in the **Security Profiles** column for the Line Manager role.

   The check mark confirms that security profiles are assigned to the role.

### Assigning Abstract and Data Roles to HCMUser Implementation User

#### Creating a Role Mapping for Implementation Data Roles: Procedure

You create a role mapping to enable you to provision the implementation data roles to implementation users, such as HCMUser. This topic describes how to create the role mapping.

**Creating the Role Mapping**

Sign in as the TechAdmin user.
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 HCM Role Provisioning Rules task.

   The Manage Role Mappings page opens.

3. In the Search Results section of the Manage Role Mappings page, click **Create**.

   The Create Role Mapping page opens.

4. In the **Mapping Name** field, enter Requestable Roles.

5. In the Conditions section, set **Assignment Status** to Active.

6. In the Associated Roles section, add a row.

7. In the **Role Name** field, search for and select the HRAnalyst_ViewAll HCM data role.

8. Select the **Requestable** option.

   Ensure that the **Self-Requestable** and **Autoproduction** options aren't selected.

---

**Note**

If **Autoproduction** is selected automatically, then deselect it.

---

9. Repeat steps 7 and 8 for the remaining roles:

   - HCMApplicationAdministrator_ViewAll
   - HRSpecialist_ViewAll

10. If you created any of the following roles, then repeat steps 7 and 8 for each one:

    - CompensationAdmin_ViewAll
    - CompensationMgr_ViewAll
    - PayrollAdmin_ViewAll
    - PayrollMgr_ViewAll

11. Click **Save and Close**. On the Manage Role Mappings page, click **Done**.

---

**Important**

When your implementation is complete, you're recommended to delete this role mapping to prevent application users from provisioning these roles.
Assigning Abstract and Data Roles to HCMUser in Oracle Identity Manager: Procedure

The implementation user HCMUser has some job roles that were assigned when the user was created. This topic explains how to assign abstract and HCM data roles to enable HCMUser to complete the functional implementation.

Accessing Oracle Identity Manager Delegated Administration

You assign additional roles to HCMUser on the Oracle Identity Manager - Delegated Administration page. Follow these steps to open the page:

1. Sign in to the Oracle HCM Cloud service environment using the OIMAdmin user name and password. If this is the first use of this user name, then you’re prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the password, the challenge questions, and their answers. You use the updated password whenever you sign in as this user subsequently.

2. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.

3. On the All Tasks tab of the Overview page, search for and select the Create Implementation Users task. The Oracle Identity Manager - Self Service page opens.

4. On the Oracle Identity Manager - Self Service page, click Administration in the top-right corner. The Oracle Identity Manager - Delegated Administration page opens.

Assigning Roles to HCMUser

1. In the Users section of the Oracle Identity Manager - Delegated Administration page, select Advanced Search - Users. The Advanced Search - Users page opens.

2. In the User Login field in the Advanced Search section, enter HCMUser and click Search.

3. In the search results, click the HCMUser link in the Display Name column. The user page for HCMUser opens.

4. On the user page, click the Roles tab. These roles already appear in the list of roles assigned to HCMUser:
   - All Users
   - Application Administrator
   - Application Implementation Consultant
   - Application Diagnostics Regular User
5. Click **Assign**.

The **Add Role** dialog box opens.

6. In the **Add Role** dialog box, search for and select the following abstract and HCM data roles:

- Employee
- Contingent Worker
- Line Manager
- HRSpecialist_ViewAll
- HRAnalyst_ViewAll
- HCMAplicationAdministrator_ViewAll

If you have licensed the relevant cloud services and created these HCM data roles, then select the roles for HCMUser:

- CompensationAdmin_ViewAll
- CompensationMgr_ViewAll
- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll

Click **Add** to add the selected roles to HCMUser.

HCMUser now has between 11 and 15 roles, depending on the cloud services that you have licensed.

**Tip**

If you add a role by mistake, you can select it and click **Revoke**.

7. Click **Close Single Tab** to close the user tab for HCMUser.

8. Close the Oracle Identity Manager Delegated Administration Console.

9. Run the Retrieve Latest LDAP Changes process to make these changes available in Oracle Fusion Human Capital Management.

**Verifying HCMUser Access: Procedure**

This topic explains how to verify that the HCMUser implementation user can access the functions enabled by the assigned roles.

1. Sign in to the Oracle HCM Cloud service using the HCMUser user name and password.
As this is the first use of this user name, you’re prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the new password, the challenge questions, and their answers. You use the new password whenever you sign in as this user subsequently.

2. Click Submit on the Password Management page.

3. Open the Oracle Applications Navigator. In the Navigator, verify that:
   - The Career menu appears, if you use Talent Management.
   - The Compensation menu and the My Information - Total Compensation Statements menu item appear, if you use Compensation Management.    
   - The Payroll menu appears, if you use Global Payroll or Global Payroll Interface.  

4. Sign out of the Oracle HCM Cloud service.

**Resetting the Service Administrator Sign-In Details: Procedure**

Once you have set up your implementation users, you can reset the service administrator sign-in details for the Oracle HCM Cloud service. You reset these details to avoid problems later when you’re loaded into the Oracle HCM Cloud service as an employee. This topic describes how to reset the service administrator sign-in details.

**Resetting the Service Administrator Sign-In Details**

Sign in to the Oracle HCM Cloud service using the OIMAdmin user name and password and follow these steps:

1. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.

2. Search for and select the Create Implementation Users task.
   The Oracle Identity Manager Self Service page opens.

3. Click Administration in the top-right of the page.
   The Identity Manager - Delegated Administration page opens.

4. In the Users section, select Advanced Search - Users. The Advanced Search - Users page opens.

5. In the User Login field, enter your service administrator user name, which is typically your e-mail. Your service activation mail contains this value.

6. Click Search. In the search results, select your service administrator user name in the Display Name column. The page for managing your user details opens.

7. Delete the value in the First Name field.
8. Change the value in the **Last Name** field to ServiceAdmin.
9. Delete the value in the **Email** field.
10. Change the **User Login** value to ServiceAdmin.
11. Click **Apply**.
12. Sign out of Identity Manager - Delegated Administration and close the tab.

After making these changes, you use the user name **ServiceAdmin** when signing in as the service administrator.
Preparing for Application Users

Preparing for Application Users: Overview

During implementation, you prepare your Oracle Human Capital Management Cloud service for application users. Decisions made during this phase determine how you manage users by default. Most such decisions can be overridden. However, for efficient user management, you’re recommended to configure your environment to both reflect enterprise policy and support most or all users.

Some key decisions and tasks are explained in this chapter. They include:

<table>
<thead>
<tr>
<th>Decision or Task</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether user accounts are created automatically for application users</td>
<td>User Account Creation Option: Explained</td>
</tr>
<tr>
<td>How user names are formed</td>
<td>Default User Name Format Option: Explained</td>
</tr>
<tr>
<td>How role provisioning is managed</td>
<td>User Account Role Provisioning Option: Explained</td>
</tr>
<tr>
<td>Whether user accounts are maintained automatically</td>
<td>User Account Maintenance Option: Explained</td>
</tr>
<tr>
<td>Whether and where user sign-in details are sent</td>
<td>Send User Name and Password Option: Explained</td>
</tr>
<tr>
<td>Understanding user-account password policy</td>
<td>Oracle Human Capital Management Cloud Password Policy: Explained</td>
</tr>
<tr>
<td>Ensuring that the employee, contingent worker, and line manager abstract roles are provisioned automatically</td>
<td>Provisioning Abstract Roles to Users Automatically: Procedure</td>
</tr>
</tbody>
</table>

User and Role-Provisioning Setup: Critical Choices

This topic introduces the user and role-provisioning options, which control the default management of user accounts. To set these options, perform the task
Manage Enterprise HCM Information in the Setup and Maintenance work area. Select Navigator - Tools - Setup and Maintenance. You can edit these values as necessary and specify an effective start date for changed values.

User Account Creation

The User Account Creation option controls:

- Whether user accounts are created automatically in Oracle Identity Management (OIM) when you create a person or party record
- The automatic provisioning of roles to users at account creation

This option may be of interest if:

- Some workers don't need access to Oracle Fusion Applications.
- Your existing provisioning infrastructure creates user accounts, and you plan to integrate it with Oracle Fusion Human Capital Management (HCM).

User Account Role Provisioning

Once a user account exists, users both acquire and lose roles as specified by current role-provisioning rules. For example, managers may provision roles to users manually, and the termination process may remove roles from users automatically. You can control role provisioning by setting the User Account Role Provisioning option.

User Account Maintenance

The User Account Maintenance option controls whether OIM user accounts are maintained, suspended, and reactivated automatically. By default, user accounts are suspended automatically when the user has no roles and reactivated when the user acquires roles. In addition, Oracle Fusion HCM sends some person information automatically to OIM when you update a person record.

Alternate Contact E-Mail Address

The alternate contact e-mail is an enterprise-wide e-mail that can receive user names and passwords for all OIM user accounts.

Send User Name and Password

Send User Name and Password controls whether an e-mail containing the user name and password is sent automatically when a user account is created. The e-mail may be sent to the alternate contact e-mail, the user, or the user’s line manager.

Default User Name Format

You can set the default format of user names for the enterprise to one of these values:
• Defined by Oracle Identity Management
• Party number
• Person number
• Primary work e-mail

User Account Creation Option: Explained

The User Account Creation option controls whether user accounts are created automatically in Oracle Identity Management (OIM) when you create a person or party record. It applies whether you create person and party records individually or in bulk. Use the Manage Enterprise HCM Information task to set this option.

This table describes the User Account Creation option values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| Both person and party users | User accounts are created automatically for both person and party users.  
This value is the default value. |
| Party users only        | User accounts are created automatically for party users only.  
User accounts aren't created automatically when you create HCM person records. For HCM users, account requests are held in the LDAP requests table, where they're identified as Suppressed. They're not passed to OIM. |
| None                   | User accounts aren't created automatically.  
All user account requests are held in the LDAP requests table, where they're identified as Suppressed. They're not passed to OIM. |

If user accounts:

• Are created automatically, then role provisioning occurs automatically, as specified by current role mappings when the accounts are created.

• Aren't created automatically, then role requests are held in the LDAP requests table, where they're identified as Suppressed. They're not passed to OIM.

If you disable the automatic creation of user accounts for some or all users, then you can:

• Create user accounts individually in OIM.
Link existing OIM user accounts to person and party records using the Manage User Account or Manage Users task.

Alternatively, you can use a provisioning infrastructure other than OIM to create and manage user accounts. In this case, you’re responsible for managing the interface with Oracle Fusion Human Capital Management, including any user-account-related updates.

**Default User Name Format Option: Explained**

The **Default User Name Format** option controls the default format of user names for the enterprise. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **Default User Name Format** option values.

<table>
<thead>
<tr>
<th>Format Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined by Oracle Identity Management</td>
<td>The user name follows the Oracle Identity Management (OIM) user-name policy. By default, OIM uses the person's first and last names. To make duplicate user names unique, OIM includes either the person's middle name or a random alphabetic character. To change the OIM user-name policy, Oracle HCM Cloud customers submit a service request. The OIM user-name format is used automatically unless you select a different value for the Default User Name Format option.</td>
</tr>
<tr>
<td>Party number</td>
<td>The party number is the user name.</td>
</tr>
<tr>
<td>Person number</td>
<td>The HCM person number is the user name.</td>
</tr>
<tr>
<td></td>
<td>For party users who have no person number, the party e-mail is used instead when person number is the default user name.</td>
</tr>
<tr>
<td>Primary work e-mail</td>
<td>The primary work e-mail (or party e-mail, for party users) is the user name.</td>
</tr>
</tbody>
</table>

A person’s party number, person number, or e-mail may not be available when the user account is requested. In this case, the account status is **Failed** until the value becomes available and you resubmit the request. If you run the Send Pending LDAP Requests process daily, then the request is likely to be resubmitted when the value becomes available. Alternatively, for individual requests, you can perform the Process User Account Request action on the Manage User Account page.

You can override default user names for individual users on the Create User, Edit User, and Manage User Account pages.
User Account Role Provisioning Option: Explained

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, a user may request some roles and acquire others automatically. All provisioning changes are role requests that Oracle Fusion Human Capital Management sends to Oracle Identity Management (OIM) by default. You can control what happens to role requests by setting the User Account Role Provisioning option. Use the Manage Enterprise HCM Information task to set this option.

This table describes the User Account Role Provisioning option values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>Role provisioning and deprovisioning occur for both person and party users.</td>
</tr>
<tr>
<td></td>
<td>This value is the default value.</td>
</tr>
<tr>
<td>Party users only</td>
<td>Role provisioning and deprovisioning occur for party users only.</td>
</tr>
<tr>
<td></td>
<td>For person users, role requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to OIM.</td>
</tr>
<tr>
<td>None</td>
<td>For both person and party users, role requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to OIM.</td>
</tr>
</tbody>
</table>

User Account Maintenance Option: Explained

By default, Oracle Identity Management (OIM) suspends user accounts automatically when the user has no roles and reactivates them when the user acquires roles again. In addition, Oracle Fusion Human Capital Management (Oracle Fusion HCM) sends some person information to OIM automatically when you update a person record. The User Account Maintenance option controls these actions. Use the Manage Enterprise HCM Information task to set this option.

This table describes the User Account Maintenance option values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>User accounts are maintained automatically for both person and party users.</td>
</tr>
<tr>
<td></td>
<td>This value is the default value.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Party users only   | User accounts are maintained automatically for party users only.  
For person users, account maintenance requests are held in the LDAP requests table, where they’re identified as Suppressed and not passed to OIM.  
Select this value if you maintain accounts for person users in some other way. |
| None               | For both person and party users, account maintenance requests are held in the LDAP requests table, where they’re identified as Suppressed and not passed to OIM.  
Select this value if you maintain accounts for both person and party users in some other way. |

You can maintain any OIM user account automatically, even if you created it outside Oracle Fusion Applications.

**Attributes Sent to Oracle Identity Management**

By default, the values of the following attributes are sent to OIM automatically whenever you update a person record:

- Person number
- System person type from the person’s primary assignment
- The Globally Unique Identifier (GUID) of the manager of the person’s primary assignment
- Work phone
- Work fax
- Both local and global versions of the person’s display name
- Global versions of the following name components:
  - First name
  - Middle name
  - Last name
  - Name suffix
- Both the formatted work-location address and the following components of the work-location address from the person’s primary assignment:
  - Address line 1
  - City
  - State
• Postal code
• Country code
• The person’s preferred language
• The person’s user name, if this value has changed

The application sends equivalent information for party users to OIM.
Oracle Fusion HCM sends no personally identifiable information (PII) to OIM.

Send User Name and Password Option: Explained

When Oracle Identity Management (OIM) creates a user account, it may send an e-mail containing the user name and password to a specified recipient. The Send User Name and Password option controls whether OIM sends this e-mail. Use the Manage Enterprise HCM Information task to set this option for the enterprise.

This table describes where OIM sends the user-credentials e-mail when you set Send User Name and Password to Yes.

<table>
<thead>
<tr>
<th>E-Mail Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternate contact e-mail</td>
<td>OIM sends e-mails for all new accounts in the enterprise to this single address.</td>
</tr>
<tr>
<td></td>
<td>You can specify an alternate contact e-mail when you perform the Manage Enterprise HCM Information task.</td>
</tr>
<tr>
<td>User’s primary work e-mail</td>
<td>Used if:</td>
</tr>
<tr>
<td></td>
<td>You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>The user’s primary work e-mail exists.</td>
</tr>
<tr>
<td>Primary work e-mail of the user’s line manager</td>
<td>Used if:</td>
</tr>
<tr>
<td></td>
<td>You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>The user’s primary work e-mail doesn’t exist.</td>
</tr>
<tr>
<td></td>
<td>The primary work e-mail of the user’s line manager exists.</td>
</tr>
<tr>
<td>None</td>
<td>OIM sends no e-mail if:</td>
</tr>
<tr>
<td></td>
<td>You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>The user’s primary work e-mail doesn’t exist.</td>
</tr>
<tr>
<td></td>
<td>The primary work e-mail of the user’s line manager doesn’t exist.</td>
</tr>
</tbody>
</table>
When Send User Name and Password Is No

If you set Send User Name and Password to No, then OIM sends no e-mails.

In this case, you can:

- Request e-mails for individual users on the Create User or Manage User Account page. If the user has no primary work e-mail, then OIM sends the e-mail to the user's line manager, if available. OIM doesn't send it to the alternate contact e-mail.
- Run the process Send User Name and Password E-Mail Notifications. This process sends e-mails for all users for whom e-mails haven't yet been sent. The process sends e-mails to users or their line managers. It doesn't send them to the alternate contact e-mail.

Note

E-mails containing user names and passwords are sent once only for any user.

Setting the User and Role Provisioning Options: Procedure

The user and role provisioning options control the creation and management of user accounts for the enterprise. This procedure explains how to set these options. For the typical case, where accounts are created and maintained automatically for all users, you can use the default settings.

Accessing the User and Role Provisioning Options

2. On the Enterprise page, select Edit - Update.
3. In the Update Enterprise dialog box, enter the effective date of any changes and click OK. The Edit Enterprise page opens.
4. Scroll down to the User and Role Provisioning Information section.

Setting the User Account Options

The User Account Options are:

- User Account Creation
- User Account Role Provisioning
- User Account Maintenance
- Default User Name Format

These options are independent of each other. For example, you can set User Account Creation to None and User Account Role Provisioning to Yes. The Default User Name Format value applies only to user accounts that are created automatically.
Setting E-Mail Options

The e-mail options are Send User Name and Password and Alternate Contact E-Mail Address.

1. Select a Send User Name and Password value.
2. Enter an e-mail in the Alternate Contact E-Mail Address field if:
   - Send User Name and Password is Yes.
   - All user names and passwords must be sent to this single e-mail.

   If Send User Name and Password is No or the users themselves must receive the e-mails, then leave this field blank.
3. Click Submit.

Oracle Human Capital Management Cloud Password Policy: Explained

Oracle Identity Management (OIM) defines the validation rules for user sign-in passwords.

By default, user sign-in passwords must be at least 6 characters long, start with an alphabetic character, and contain at least:

- 2 alphabetic characters
- 1 numeric character
- 1 uppercase letter
- 1 lowercase letter

In addition, passwords must not be the same as or contain the user’s:

- First name
- Last name
- User name

Password Policy Update

To change the default OIM password policy in Oracle Human Capital Management Cloud, submit a service request.

Provisioning Abstract Roles to Users Automatically: Procedure

Provisioning the employee, contingent worker, and line manager abstract roles automatically to users is efficient, as most users have at least one of these roles.
It also ensures that users have basic access to functions and data when they first sign in to Oracle Fusion Applications. This topic explains how to set up automatic role provisioning during implementation using the Manage HCM Role Provisioning Rules task.

**Provisioning the Employee Role Automatically to Employees**

1. Sign in as the TechAdmin user.
2. Select **Navigator - Tools - Setup and Maintenance** to open the Setup and Maintenance work area.
3. On the All Tasks tab, search for and select the Manage HCM Role Provisioning Rules task. The Manage Role Mappings page opens.
4. In the Search Results section of the Manage Role Mappings page, click **Create**. The Create Role Mapping page opens.
5. In the **Mapping Name** field enter Employee.
6. Complete the fields in the Conditions section of the Create Role Mapping page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

7. In the Associated Roles section of the Create Role Mapping page, add a row.
8. In the **Role Name** field of the Associated Roles section, search for and select the Employee role.
9. If **Autoprovision** isn't selected automatically, then select it.
10. Ensure that the **Requestable** and **Self-Requestable** options aren’t selected.

   Click **Save and Close**.

**Provisioning the Contingent Worker Role Automatically to Contingent Workers**

Repeat the steps in Provisioning the Employee Role Automatically to Employees, with the following changes:

1. In step 5, use Contingent Worker as the mapping name.
2. In step 6, set **System Person Type** to Contingent Worker.
3. In step 8, search for and select the Contingent Worker role.

**Provisioning the Line Manager Role Automatically to Line Managers**

1. In the Search Results section of the Manage Role Mappings page, click **Create**. The Create Role Mapping page opens.
2. In the **Mapping Name** field enter Line Manager.

3. Complete the fields in the Conditions section of the Create Role Mapping page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
<tr>
<td>Manager with Reports</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4. In the Associated Roles section of the Create Role Mapping page, add a row.

5. In the **Role Name** field of the Associated Roles section, search for and select the Line Manager role.

6. If **Autoprovision** isn't selected automatically, then select it.

7. Ensure that the **Requestable** and **Self-Requestable** options aren’t selected.

   Click **Save and Close**.

8. On the Manage Role Mappings page, click **Done**.

---

**Note**

To provision the line manager role automatically to contingent workers, follow these steps to create an additional role mapping. In step 2, use a unique mapping name (for example, Contingent Worker Line Manager). In step 3, set **System Person Type** to Contingent Worker.

---

**FAQs for Preparing for Application Users**

**Can I implement single sign-in in the cloud?**

Yes. Single sign-in enables users to sign in once but access multiple applications, including Oracle Fusion Human Capital Management.

If you’re using Oracle Human Capital Management Cloud, then you submit a service request for implementation of single sign-in.
Creating Application Users: Points to Consider

When you create person records in Oracle HCM Cloud, user accounts can be created automatically in Oracle Identity Management (OIM). The User and Role Provisioning options control whether accounts are created automatically. You set these options for the enterprise during implementation using the Manage Enterprise HCM Information task.

Some enterprises use systems other than Oracle HCM Cloud to manage user and role provisioning. In this case, you set the User and Role Provisioning options to prevent automatic creation of user accounts.

User accounts created by Oracle HCM Cloud don't provide access to other enterprise applications.

Creating Person Records

You can create person records:

- Individually, using tasks such as Hire an Employee
- By uploading them in bulk, using HCM Spreadsheet Data Loader or HCM File-Based Loader

Note

During implementation, you can also use the Create User task to create individual application users for test purposes. However, after implementation, you use tasks such as Hire an Employee and Add a Contingent Worker. These tasks are functionally rich and create the employment information required for Oracle HCM Cloud implementations. Don't use Create User, which is intended primarily for Oracle Fusion Applications customers who aren't implementing Oracle HCM Cloud.

Uploading Person Records Using HCM Spreadsheet Data Loader

You can upload person records in bulk using HCM Spreadsheet Data Loader.

- During implementation, you use the task Initiate HCM Spreadsheet Load. Select Navigator - Tools - Setup and Maintenance and search for the task Initiate HCM Spreadsheet Load.
- After implementation, you can use the task Initiate Spreadsheet Load. Select Navigator - Workforce Management - Data Exchange and select the task Initiate Spreadsheet Load.
Both tasks open the Initiate Spreadsheet Load page, where you select the Create Worker spreadsheet.

HCM Spreadsheet Data Loader is easy to use. It's suitable for loading simple person records (for example, records without date-effective assignment history) in small-to-medium volumes.

When you upload person records using HCM Spreadsheet Data Loader, requests for user accounts are created automatically, depending on the User and Role Provisioning options. You run the process Send Pending LDAP Requests to send these bulk requests for user accounts to OIM.

Uploading Person Records Using HCM File-Based Loader

HCM File-Based Loader is suitable for uploading very large numbers of person records or very complex person records that you can't load using HCM Spreadsheet Data loader. For more information about HCM File-Based Loader, see the File-Based Loader User's Guide on My Oracle Support (MOS Document ID 1595283.1).

When you upload person records using HCM File-Based Loader, requests for user accounts are created automatically, depending on the User and Role Provisioning options. You run the process Send Pending LDAP Requests to send these bulk requests for user accounts to OIM.

Creating Oracle HCM Cloud Users Using the New Person Tasks: Procedure

Once your initial implementation of Oracle Human Capital Management Cloud (Oracle HCM Cloud) is complete, you create person records:

- Individually, using tasks such as Hire an Employee in the New Person work area
- In bulk, by uploading person records using HCM Spreadsheet Data Loader or HCM File-Based Loader.

This topic summarizes how to create person records using the Hire an Employee task, with emphasis on any steps that affect user and role provisioning.

Hiring an Employee

You must have the Human Resource Specialist or Line Manager job role to hire an employee. Follow these steps:

1. Select Navigator - Person Management - New Person to open the New Person work area.
2. In the Tasks pane, select Hire an Employee. The Hire an Employee: Identification page opens.
3. If the Person Number value is Generated automatically, then the number is generated on approval of the hire. If the field is blank, then you can enter a person number.

The user name is the person number if the Default User Name Format option for the enterprise is person number.

By default, the user name is based on the person's first and last names, which you enter here.

5. A user can have only one work e-mail. If you enter a value here, then it’s sent to Oracle Identity Management (OIM). Once the person record exists, you manage the e-mail in OIM. If you enter no work e-mail, then the e-mail is both created automatically and managed in OIM. You can’t edit the work e-mail in Oracle HCM Cloud.

   The user name is the work e-mail if the Default User Name Format option for the enterprise is primary work e-mail.


7. Many assignment details, including Assignment Status and Job, may occur as conditions in role mappings. For example, users may acquire a role automatically if their grade matches that in the associated role mapping.

8. Click Next. The Hire an Employee: Roles page opens.

   Any roles for which the employee qualifies automatically appear in the Role Requests region.

9. To add roles manually, click Add Role. The Add Role dialog box opens.

10. Search for and select the role.

    Tip

    Roles that you can provision to others appear in a role mapping for which you satisfy the role-mapping conditions and where the Requestable option is selected for the role.

    The role appears in the Role Requests region with the status Add requested.

    Repeat steps 9 and 10 for additional roles.


    This action:
    • Submits the Hire an Employee transaction for approval
    • Creates a request for OIM to create the user account and provision the requested roles, on approval of the hire

    If the sending of user names and passwords is enabled, then an e-mail is sent to either the enterprise e-mail or the user.

Creating Oracle HCM Cloud Users Using the Create User Task:

Procedure

During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a
user account. After implementation, you use tasks such as Hire an Employee to create application users. The Create User task isn’t recommended once implementation is complete. This topic describes how to create a test user using the Create User task.

To perform Create User, you must have the human resource specialist job role. Sign in and follow these steps:

1. Select **Navigator - Manager Resources - Manage Users** to open the Manage Users page.
2. In the Search Results section, click **Create**. The Create User page opens.

**Completing Personal Details**

1. Enter the user’s name.
2. In the **E-Mail** field, enter the user’s primary work e-mail.
3. In the **Hire Date** field, enter the hire date for a worker. For other types of users, enter a user start date. You can’t edit this date once the user exists.

**Completing User Details**

You can enter a user name for the user. If you leave the **User Name** field blank, then the user name follows the enterprise default user-name format.

**Setting User Notification Preferences**

The **Send user name and password** option controls whether an e-mail containing the user name and a temporary password is sent when the account is created. This option is selected by default if these e-mails are enabled for the enterprise.

When the **Send user name and password** option is selected, the e-mail is sent to:

1. The enterprise e-mail, if it exists and sending of e-mails is enabled for the enterprise.
2. The user, if no enterprise e-mail exists.
3. The user’s line manager, if the user’s e-mail doesn’t exist.

If none of these e-mails exists, then no e-mail is sent.

If you deselect this option, then you can send the e-mail later by running the process **Send User Name and Password E-Mail Notifications**.

**Completing Employment Information**

1. Select a **Person Type** value.
2. Select **Legal Employer** and **Business Unit** values.

**Completing Resource Information**

This section doesn’t apply to Oracle HCM Cloud users.
Adding Roles

1. Click **Autoprovision Roles**. Any roles for which the user qualifies automatically appear in the Role Requests table.

2. To provision a role manually to the user, click **Add Role**. The Add Role dialog box opens.

3. Search for and select the role.

---

**Tip**

Roles that you can provision to others appear in a role mapping for which you satisfy the role-mapping conditions and where the **Requestable** option is selected for the role.

The role appears in the Role Requests region with the status **Add requested**. The role request is sent to Oracle Identity Management (OIM) when you click **Save and Close**.

Repeat steps 2 and 3 for additional roles.

4. Click **Save and Close**.

5. Click **Done**.

---

**FAQs for Creating Application Users**

**How can I create a user account for a new worker?**

When you create a person record, a user account is created automatically in Oracle Identity Management (OIM) if automatic creation of accounts is enabled. Otherwise, you can create accounts directly in OIM, for example.

If user accounts already exist in OIM, then you can link them to person records on the Manage User Account page.

**How do I create a user account for an existing worker?**

On the Manage User Account page, select **Create User Account**. Update account details, if appropriate, and click **Save**.

Once Oracle Identity Management (OIM) processes the request successfully, the account becomes available.

---

**Note**

If automatic creation of accounts is disabled, you can’t use the Create User Account action. Instead, create accounts directly in OIM, for example.
Where do default user names come from?

By default, user names are defined in Oracle Identity Management (OIM). The format is typically the user's first and last names, but this format can be changed in OIM.

The OIM format can also be overridden for the enterprise in Oracle Fusion HCM. Your enterprise may be using person number, party number, or primary work e-mail in place of the OIM format.

Why did some roles appear automatically?

Roles appear automatically for a user when:

- The user's assignment attributes, such as person type and job, match the conditions specified for the role in a role mapping.
- In the role mapping, the role has the Autoprovision option selected.
Managing User Accounts: Procedure

Human resource specialists (HR specialists) can manage user accounts for users whose records they can access. This topic describes how to update a user account.

To access the user account page for a person:

1. Select **Navigator - Workforce Management - Person Management** to open the Search Person page.
2. Search for and select the person whose account you’re updating. The Person Management work area opens.
3. In the Tasks pane, click **Manage User Account**. The Manage User Account page opens.

Managing User Roles

To add a role:

1. Click **Add Role**.

The Add Role dialog box opens.
2. In the **Role Name** field, search for the role that you want to add.
3. In the search results, select the role and click **OK**.

The role appears in the Role Requests region with the status **Add Requested**.
4. Click **Save**.

To remove a role from any section of this page:

1. Select the role and click **Remove**.
2. In the **Warning** dialog box, click **Yes** to continue.
3. Click **Save**.
Clicking **Save** sends requests to add or remove roles to Oracle Identity Management (OIM). Requests to add roles appear in the Role Requests in the Last 30 Days section. Once provisioned, roles appear in the Current Roles section.

To update a user’s roles automatically, select **Actions - Autoprovion Roles**. This action applies to roles for which the Autoprovion option is selected in all current role mappings. The user immediately:

- Acquires any role for which he or she qualifies but doesn’t currently have
- Loses any role for which he or she no longer qualifies

You’re recommended to autoprovion roles for individual users if you know that additional or updated role mappings exist for which those users qualify.

**Copying Personal Data to LDAP**

By default, changes to personal data, such as person name and phone, are copied to the OIM LDAP directory periodically. To copy any changes to LDAP immediately:

1. Select **Actions - Copy Personal Data to LDAP**.
2. In the Copy Personal Data to LDAP dialog box, click **Overwrite LDAP**.

**Resetting Passwords**

To reset a user’s password:

1. Select **Actions - Reset Password**.
2. In the **Warning** dialog box, click **Yes** to continue.

   This action sends a temporary password to the user’s primary work e-mail.

**Editing User Names**

To edit a user name:

1. Select **Actions - Edit User Name**.
2. In the Update User Name dialog box, enter the user name and click **OK**.
3. Click **Save**.

This action sends the updated user name to OIM. Once OIM has processed the request, the user can sign in using the updated name. As the user receives no automatic notification of the change, you’re recommended to send the details to the user.

**Tip**

Users can perform any of these account-management tasks for themselves by selecting **Navigator - My Information - My Account**. However, they may not be able to request the roles that another user, such as an HR specialist, can provision to them.
Changing User Names: Explained

By default, user names are generated automatically in the enterprise default format when you create a person record. You can change user names for existing HCM users, and users can change their own user names. This topic describes the automatic generation of user names and explains how to change an existing user name.

User Names When Creating Users

You create an HCM user by selecting a task, such as Hire an Employee, in the New Person work area. The user name is generated automatically in the enterprise default format. This table summarizes the effects of the default formats.

<table>
<thead>
<tr>
<th>Default User-Name Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined by Oracle Identity Management (OIM)</td>
<td>OIM generates the user name, typically using first and last names.</td>
</tr>
</tbody>
</table>
| Person number                  | If your enterprise uses manual numbering, then any number that you enter becomes the user name.  
                                | Otherwise, the number is generated automatically and you can't edit it. The automatically generated number becomes the user name. |
| Work e-mail                    | If you enter a work e-mail, that value becomes the user name. Otherwise, the work e-mail that OIM defines becomes the user name. |

Existing User Names

You can change an existing user name on the Manage User Account page. Select Navigator - Workforce Management - Person Management. In the Person Management work area, select Manage User Account, then Actions - Edit User Name.

Users can request a change for themselves by selecting Navigator - My Information - My Account, then Actions - Edit User Name.

The updated name, which can be in any format, is sent automatically to OIM. When you change an existing user name, the user’s password and roles remain the same. The user receives no automatic notification of the change. Therefore, you’re recommended to send details of the updated user name to the user.

Sending Personal Data to LDAP: Explained

Oracle Identity Management (OIM) maintains Lightweight Directory Access Protocol (LDAP) user accounts for users of Oracle Fusion Applications. By
default, Oracle Fusion HCM (HCM) sends some personal information about users to OIM. This information includes the person number, person name, phone, and manager of the person’s primary assignment. HCM sends these details to OIM to ensure that HCM and OIM hold the same information about users.

This topic describes how and when you can send personal information explicitly to OIM.

**Bulk Creation of Users**

After loading person records using Oracle Fusion HCM File-Based Loader or HCM Spreadsheet Data Loader, for example, you run the process Send Pending LDAP Requests. This process sends bulk requests for user accounts to OIM.

When you load person records in bulk, the order in which they’re created in HCM is undefined. Therefore, a person’s record may exist before the record for his or her manager. In such cases, the Send Pending LDAP Requests process sends no manager details for the person to OIM. The OIM information therefore differs from the information that HCM holds for the person. To correct any differences between the OIM and HCM versions of personal details, you run the process Send Personal Data for Multiple Users to LDAP.

**The Send Personal Data for Multiple Users to LDAP Process**

Send Personal Data for Multiple Users to LDAP updates OIM information to match that held by HCM. You run the process for either all users or changed users only, as described in this table.

<table>
<thead>
<tr>
<th>User Population</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users</td>
<td>The process sends personal details for all users to OIM, regardless of whether they have changed since personal details were last sent to OIM.</td>
</tr>
<tr>
<td>Changed users only</td>
<td>The process sends only personal details that have changed since details were last sent to OIM (regardless of how they were sent). This option is the default setting.</td>
</tr>
</tbody>
</table>

**Note**

If User Account Maintenance is set to **No** for the enterprise, then the process doesn’t run.

The process doesn’t apply to party users.

You must have the IT Security Manager or Human Capital Management Application Administrator role to run this process.

**The Copy Personal Data to LDAP Action**

From the Manage User Account page, you can copy personal data to OIM for an individual user. By default, personal data changes are copied periodically
to OIM. However, this action is available for you to copy changes to OIM immediately, if necessary.

**Processing a User Account Request: Explained**

This topic describes the Process User Account Request action, which may appear on the Manage User Account page for users who have no user account.

**The Process User Account Request Action**

The Process User Account Request action is available when the status of the worker’s user account is either Requested or Failed. These values indicate that the account request hasn’t completed.

Selecting this action submits the request to Oracle Identity Management (OIM) again. Once the request completes successfully, the account becomes available to the user. Depending on your enterprise setup, the user may receive an e-mail containing the user name and password.

**Role Provisioning**

Any roles that the user will have appear in the Roles section of the Manage User Account page. You can add or remove roles before selecting the Process User Account Request action. If you make changes to roles, you must click **Save**.

**The Send Pending LDAP Requests Process**

The Process User Account Request action has the same effect as the Send Pending LDAP Requests process. If Send Pending LDAP Requests runs automatically at intervals, then you can wait for that process to run if you prefer. Using the Process User Account Request action, you can submit user-account requests immediately for individual workers.

**Suspending User Accounts: Explained**

You can’t delete a user account. However, user accounts are suspended automatically when a user has no roles and reactivated automatically when roles are provisioned again. You can also suspend a user account manually, if necessary. This topic describes how automatic account suspension occurs and explains how to suspend a user account manually.

**Work Relationship Termination**

When you terminate a work relationship:

- The user loses any automatically provisioned roles for which he or she no longer qualifies. This deprovisioning is automatic.
- If the user has no other active work relationships, then the user also loses manually provisioned roles. These are:
  - Roles that he or she requested
• Roles that another user, such as a line manager, provisioned to the user

If the user has other, active work relationships, then he or she keeps any manually provisioned roles.

When terminating a work relationship, you specify whether the user is to lose roles on the day following termination or when the termination is approved.

A terminated worker’s user account is suspended automatically at termination only if he or she has no roles. Users can acquire roles automatically at termination, if an appropriate role mapping exists. In this case, the user account remains active.

**Reenabling of User Accounts**

If you rehire a worker or reverse the termination of a work relationship, then:

• The user regains any role that he or she lost automatically at termination.

  If you removed any roles from the user manually at termination, then you must restore them to the user manually, if required.

• The user loses any role that he or she acquired automatically at termination.

• If the user account was suspended automatically at termination, then it’s automatically reenabled.

You can apply autoprovisioning on the Manage User Account page to update the automatic provisioning of roles for a rehired or reinstated worker.

**Manual Suspension of User Accounts**

To suspend a user account manually, edit the user account. Select **Navigator - Manager Resources - Manage Users**. On the Edit User page, set the **User Account Status** value to **Inactive**.

**FAQs for Managing Application Users**

**What happens when I autoprovision roles for a user?**

The role-provisioning process reviews the user’s assignments against all current role mappings.

The user immediately:

• Acquires any role for which he or she qualifies but doesn’t have

• Loses any role for which he or she no longer qualifies

You’re recommended to autoprovision roles to individual users on the Manage User Account page when new or changed role mappings exist. Otherwise, no automatic updating of roles occurs until you next update the user’s assignments.
Why is the user losing roles automatically?

The user acquired these roles automatically based on his or her assignment information. Changes to the user's assignments mean that the user is no longer eligible for these roles. Therefore, the roles no longer appear.

If a deprovisioned role is one that you can provision manually to users, you can reassign the role to the user, if appropriate.

Why can't I see the roles that I want to provision to a user?

You can provision a role if a role mapping exists for the role, the Requestable option is selected for the role in the role mapping, and at least one of your assignments satisfies the role-mapping conditions. Otherwise, you can't provision the role to other users.

What happens if I deprovision a role from a user?

The user loses the access to functions and data that the removed role was providing exclusively. The user becomes aware of the change when he or she next signs in.

If the user acquired the role automatically, future updates to the user's assignments may mean that the user acquires the role again.

What's a delegated role?

A job, abstract, or data role that a user, known as the delegator, assigns to another user, known as the proxy user.

You can delegate a role for a specified period, such as a planned absence, or indefinitely.

What happens if I revoke user access from a person with multiple work relationships?

The person loses roles provisioned automatically for assignments in this work relationship only.

The person keeps roles that he or she:

• Requested or another user provisioned manually.
  Deprovision these roles manually, if necessary.
• Acquired automatically for other work relationships.

If the person has roles at termination, the user account remains active. Otherwise, it's suspended automatically.

**Why does this person have no user account?**

Automatic creation of user accounts may be disabled. In this case, you create accounts directly in Oracle Identity Management (OIM), for example.

You can link an existing OIM user account to the worker on the Manage User Account page. This action may be necessary if the account was created automatically but a problem occurred before a link to the worker was established.

**What happens when I link a user account?**

The request to link the person or party record to the account goes automatically to Oracle Identity Management. Once the account status is **Active**, current roles appear in the Roles section of the Manage User Account or Edit User page, and the user can sign in. You're recommended to notify the user when the account is linked.

**What happens if I edit a user name?**

The updated user name is sent to Oracle Identity Management (OIM) for processing when you click **Save** on the Manage User Account or Edit User page. The account status remains **Active**, and the user's roles and password are unaffected. As the user isn't notified automatically of the change, you're recommended to notify the user.

**What happens when I copy personal data to LDAP?**

Oracle Identity Management (OIM) holds some personal information about users, such as name, work phone, and work location address. Changes to personal information in Oracle Fusion Human Capital Management are copied automatically at intervals to OIM. To send any changes to OIM immediately, you can perform the Copy Personal Data to LDAP action. This action is optional.

**What happens if I send the user name and password?**

The user name and password go to the primary work e-mail of the user or user's line manager, if any.
You can send these details once only for any user. If you deselect this option on the Manage User Account or Create User page, you can send the details later. To do this, run the process Send User Name and Password E-Mail Notifications.

**What happens if I reset a user’s password?**

A new, temporary password is sent to the user’s primary work e-mail address.

**How can I notify users of their user names and passwords?**

You can run the process Send User Name and Password E-Mail Notifications from the Scheduled Processes work area. For users for whom you haven’t so far requested an e-mail, this process resets passwords and sends out user names and passwords. The e-mail goes to the primary work e-mail of the user or the user’s line manager. You can send the user name and password once only to any user.
Provisioning Roles to Application Users

Role Mappings: Explained

Roles provide user access to data and functions. To provision a role to users, you define a relationship, called a role mapping, between the role and some conditions. You provision all types of roles using role mappings. This topic describes role mappings for automatic and manual role provisioning. Use the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area.

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

- At least one of the user’s assignments matches all role-mapping conditions.
- You select the Autoprovision option for the role in the role mapping.

For example, for the data role Sales Manager Finance Department, you could select the Autoprovision option and specify the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Finance Department</td>
</tr>
<tr>
<td>Job</td>
<td>Sales Manager</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

Users with at least one assignment that matches these conditions acquire the role automatically when you create or update the assignment. The provisioning process also removes automatically provisioned roles from users who no longer satisfy the role-mapping conditions.

Note

Automatic provisioning of roles to users is a request to Oracle Identity Management (OIM) to provision the role. OIM may reject the request if it fails a custom OIM approval process, for example.
Manual Provisioning of Roles to Users

Users such as line managers can provision roles manually to other users if:

- At least one of the assignments of the user who’s provisioning the role (for example, the line manager) matches all role-mapping conditions.
- You select the Requestable option for the role in the role mapping.

For example, for the data role Training Team Leader, you could select the Requestable option and specify the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager with Reports</td>
<td>Yes</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

Any user with at least one assignment that matches both conditions can provision the role Training Team Leader manually to other users.

Users keep manually provisioned roles until either all of their work relationships are terminated or you deprovision the roles manually.

Role Requests from Users

Users can request a role when managing their own accounts if:

- At least one of their assignments matches all role-mapping conditions.
- You select the Self-requestable option for the role in the role mapping.

For example, for the data role Expenses Reporter you could select the Self-requestable option and specify the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>ABC Department</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

Any user with at least one assignment that matches these conditions can request the role. The user acquires the role either immediately or after approval. Self-requested roles are defined as manually provisioned.

Users keep manually provisioned roles until either all of their work relationships are terminated or you deprovision the roles manually.

Role-Mapping Names

Role mapping names must be unique in the enterprise. Devise a naming scheme that shows the scope of each role mapping. For example, the role mapping Autoprovisioned Roles Sales could include all roles provisioned automatically to workers in the sales department.
Creating a Role Mapping: Procedure

To provision roles to users, you create role mappings. This topic explains how to create a role mapping.

Sign in as IT Security Manager 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 task **Manage HCM Role Provisioning Rules**.
   - The Manage Role Mappings page opens.

3. In the Search Results section of the page, click **Create**.
   - The Create Role Mapping page opens.

**Defining the Role-Mapping Conditions**

Values in the Conditions section determine when the role mapping applies. For example, these values limit the role mapping to current employees of the Procurement Department in Denver whose Job is Chief Buyer.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Procurement Department</td>
</tr>
<tr>
<td>Job</td>
<td>Chief Buyer</td>
</tr>
<tr>
<td>Location</td>
<td>Denver</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

Users must have at least one assignment that meets all of these conditions.

**Identifying the Roles**

1. In the Associated Roles section, click **Add Row**.

2. In the **Role Name** field, search for and select the role that you’re provisioning. For example, search for the data role **Procurement Analyst Denver**.

3. Select one or more of the role-provisioning options:

<table>
<thead>
<tr>
<th>Role-Provisioning Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestable</td>
<td>Qualifying users can provision the role to other users.</td>
</tr>
</tbody>
</table>
### Role- Provisioning Option

<table>
<thead>
<tr>
<th>Role-Provisioning Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Requestable</td>
<td>Qualifying users can request the role for themselves.</td>
</tr>
<tr>
<td>Autoprovision</td>
<td>Qualifying users acquire the role automatically.</td>
</tr>
</tbody>
</table>

Qualifying users have at least one assignment that matches the role-mapping conditions.

**Important**

Autoprovision is selected by default. Remember to deselect it if you don’t want autoprovisioning.

The **Delegation Allowed** option indicates whether users who have the role or can provision it to others can also delegate it. You can’t change this value, which is part of the role definition. When adding roles to a role mapping, you can search for roles that allow delegation.

4. If appropriate, add more rows to the Associated Roles section and select provisioning options. The role-mapping conditions apply to all roles in this section.

5. Click **Save and Close**.

**Important**

The **Apply Autoprovisioning** action on the Create Role Mapping and Edit Role Mapping pages evaluates all users in the enterprise against the criteria in the role mapping. Therefore, multiple role requests may be sent to Oracle Identity Management (OIM). If you apply autoprovisioning repeatedly in a short period, then the number of role requests sent to OIM can cause performance issues. To avoid these issues, you’re recommended to identify a single user to apply autoprovisioning during nonpeak times.

---

**Role Mappings: Examples**

You must provision roles to users either automatically or manually. This topic provides some examples of typical role mappings to support automatic and manual role provisioning.

**Creating a Role Mapping for Employees**

All employees must have the Employee role automatically from their hire dates. In addition, the few employees who claim expenses must be able to request the Expenses Reporting data role.

You create a role mapping called All Employees and enter the following conditions.
In the role mapping you include the:

- Employee role, and select the **Autoprovision** option
- Expenses Reporting role, and select the **Self-requestable** option

### Creating a Role Mapping for Line Managers

Any type of worker can be a line manager in the sales business unit. You create a role mapping called Line Manager Sales BU and enter the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>Sales</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Active</td>
</tr>
<tr>
<td>Manager with Reports</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You include the Line Manager role and select the **Autoprovision** option. Any worker with at least one assignment that matches the role-mapping conditions acquires the role automatically.

In the same role mapping, you can include roles that line managers can:

- Provision manually to other users.
  - You select the **Requestable** option for these roles.
- Request for themselves.
  - You select the **Self-requestable** option for these roles.

### Creating a Role Mapping for Retirees

Retired workers have system access to manage their retirement accounts. You create a role mapping called All Retirees and enter the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Person Type</td>
<td>Retiree</td>
</tr>
<tr>
<td>Assignment Status</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

You include the custom role Retiree in the role mapping and select the **Autoprovision** option. When at least one of a worker's assignments satisfies the role-mapping conditions, he or she acquires the role automatically.
Role Provisioning and Deprovisioning: Explained

You must provision roles to users. Otherwise, they have no access to data or functions and can't perform application tasks. This topic explains how role mappings control role provisioning and deprovisioning. Use the Manage HCM Role Provisioning Rules task to create role mappings.

Role Provisioning Methods

You can provision roles to users:

- Automatically
- Manually
  - Users such as line managers can provision roles manually to other users.
  - Users can request roles for themselves.

For both automatic and manual role provisioning, you create a role mapping to specify when a user becomes eligible for a role.

Role Types

You can provision both predefined and custom data roles, abstract roles, and job roles to users.

Automatic Role Provisioning

Users acquire a role automatically when at least one of their assignments satisfies the conditions in the relevant role mapping. Provisioning occurs when you create or update worker assignments.

For example, when you promote a worker to a management position, the worker acquires the line manager role automatically if an appropriate role mapping exists. All changes to assignments cause review and update of a worker’s automatically provisioned roles.

Role Deprovisioning

Users lose automatically provisioned roles when they no longer satisfy the role-mapping conditions. For example, a line manager loses an automatically provisioned line manager role when he or she stops being a line manager.

You can also manually deprovision automatically provisioned roles at any time.

Users lose manually provisioned roles automatically only when all of their work relationships are terminated. Otherwise, users keep manually provisioned roles until you deprovision them manually.

Roles at Termination

When you terminate a work relationship, the user automatically loses all automatically provisioned roles for which he or she no longer qualifies. The user loses manually provisioned roles only if he or she has no other work.
relationships. Otherwise, the user keeps manually provisioned roles until you remove them manually.

The user who’s terminating a work relationship specifies when the user loses roles. Deprovisioning can occur:

- As soon as the termination is submitted or approved
- On the day after the termination date

Role mappings can provision roles to users automatically at termination. For example, a terminated worker could acquire the custom role Retiree at termination based on assignment status and person type values.

Reversing a termination reinstates any roles that the user lost automatically at termination and removes any that the user acquired automatically at termination.

Date-Effective Changes to Assignments

Automatic role provisioning and deprovisioning are based on current data. For a future-dated transaction, such as a future promotion, role provisioning occurs on the day the changes take effect. The Send Pending LDAP Requests process identifies future-dated transactions and manages role provisioning and deprovisioning at the appropriate time.

These role-provisioning changes take effect on the system date. Therefore, a delay of up to 24 hours may occur before users in other time zones acquire their roles.

Applying Autoprovisioning: Explained

Autoprovisioning is the automatic allocation or removal of user roles. It occurs automatically for individual users when you create or update assignments. You can also apply autoprovisioning explicitly for the enterprise using the Manage HCM Role Provisioning Rules task. This topic explains the effects of applying autoprovisioning for the enterprise.

Roles Affected by Autoprovisioning

Autoprovisioning applies only to roles that have the Autoprovision option enabled in a role mapping.

It doesn't apply to roles without the Autoprovision option enabled. For example, autoprovisioning doesn't affect roles with only the Requestable option enabled.

The Apply Autoprovisioning Action

When you apply autoprovisioning in a role mapping, the process compares all current user assignments with all current role mappings.

- Users with at least one assignment that matches the conditions in a role mapping and who don’t currently have the associated roles acquire those roles.
- Users who currently have the roles but no longer satisfy the associated role-mapping conditions lose those roles.
If this deprovisioning leaves a user without roles, then that user's account is also suspended automatically.

Automatic provisioning and deprovisioning of roles occurs immediately.

**Important**

The Apply Autoproposition action isn't limited to the current role mapping. The process applies to all current role mappings. Therefore, you must avoid applying autoprovisioning more than once in any day. Otherwise, the number of role requests generated each time you apply autoprovisioning slows the provisioning process.

**Autoproposition for Individual Users**

You can apply autoprovisioning for individual users on the Manage User Account page.

### Role Status Values: Explained

When you search for a role on the Manage Data Role and Security Profiles page, the role's status appears in the search results. This topic explains the role status values.

**Role Status Values and Their Meanings**

This table shows role status values and their meanings.

<table>
<thead>
<tr>
<th>Status Value</th>
<th>Meaning</th>
<th>Role Can Be Provisioned to Users?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>This HCM data role exists in Oracle Identity Management (OIM).</td>
<td>Yes</td>
</tr>
<tr>
<td>Failed</td>
<td>A request to create an HCM data role failed.</td>
<td>No</td>
</tr>
<tr>
<td>In progress with Oracle Identity Management</td>
<td>OIM received a request to create an HCM data role but processing hasn’t yet started.</td>
<td>No</td>
</tr>
<tr>
<td>Predefined</td>
<td>The HCM data role, abstract role, or job role is predefined in Oracle Fusion Applications and exists in OIM.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rejected</td>
<td>The request to create an HCM data role was rejected.</td>
<td>No</td>
</tr>
<tr>
<td>Requested</td>
<td>The request to create an HCM data role hasn't yet reached OIM.</td>
<td>No</td>
</tr>
</tbody>
</table>
Role Provisioning Status Values: Explained

The status value of a role request describes the request’s progress. This topic describes the request status values, which appear on the Manage User Account, New Person Roles, Create User, and Edit User pages.

Role Provisioning Status Values and Their Meanings

This table describes status values for role provisioning requests.

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>The request completed successfully. The user has the role.</td>
</tr>
<tr>
<td>Failed</td>
<td>The request failed, and the role wasn’t provisioned to the user. The associated error message provides more information.</td>
</tr>
<tr>
<td>Partially complete</td>
<td>The request is in progress.</td>
</tr>
<tr>
<td>Pending</td>
<td>Oracle Identity Management (OIM) received the request but processing hasn’t yet started.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The request was rejected, and the role wasn’t provisioned to the user. An associated error message may provide more information.</td>
</tr>
<tr>
<td>Requested</td>
<td>The request was made but OIM hasn’t yet acknowledged it.</td>
</tr>
<tr>
<td>SOD checks in progress</td>
<td>Segregation- of-duties checks are in progress. The name of any conflicting role that the user already has appears in the Conflicting Role column.</td>
</tr>
<tr>
<td>SOD checks rejected</td>
<td>The request failed segregation- of-duties checks, and the role wasn’t provisioned to the user. The associated error message provides more information. The name of any conflicting role that the user already has appears in the Conflicting Role column.</td>
</tr>
<tr>
<td>SOD remediation in progress</td>
<td>Processing to remove segregation- of-duties conflicts is in progress.</td>
</tr>
<tr>
<td>SOD remediation rejected</td>
<td>Attempts to remove segregation- of-duties conflicts were rejected. The associated error message provides more information. The name of any conflicting role that the user already has appears in the Conflicting Role column.</td>
</tr>
</tbody>
</table>
FAQs for Provisioning Roles to Application Users

What happens if I edit a role mapping?

You’re recommended to apply autoprovisioning immediately from the role mapping to implement your changes. Otherwise, updating of roles for a user occurs only when a human resource specialist or line manager:

- Updates the user’s assignments
- Autoprovisions roles for the user on the Manage User Account or Edit User page

**Note**

If you edit more than one role mapping, apply autoprovisioning once when you have edited them all.

What’s a role-mapping condition?

Most are assignment attributes. At least one of a user’s assignments must match all assignment values that you specify in the role mapping if the user is to qualify for the associated roles.

What’s an associated role in a role mapping?

Any role that you want to provision to users. Such roles can include Oracle Fusion Applications predefined roles, custom roles, and HCM data roles.

What’s the provisioning method?

The provisioning method identifies how the user acquired the role. This table describes its values.

<table>
<thead>
<tr>
<th>Provisioning Method</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic</td>
<td>The user qualifies for the role automatically based on his or her assignment attribute values.</td>
</tr>
<tr>
<td>Manual</td>
<td>Either another user assigned the role to the user, or the user requested the role.</td>
</tr>
<tr>
<td>Provisioning Method</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>External</td>
<td>The user acquired the role outside Oracle Fusion Human Capital Management.</td>
</tr>
</tbody>
</table>
HCM Data Roles and Security Profiles

HCM Data Roles: Explained

HCM data roles combine a job role with the data that users with the role must access. You identify the data in security profiles. As data roles are specific to the enterprise, no predefined HCM data roles exist.

To create an HCM data role, you must have the IT Security Manager job role. You perform the task Manage Data Role and Security Profiles (Navigator - Tools - Setup and Maintenance - Manage Data Role and Security Profiles).

Job Role Selection

When you create an HCM data role, you include a job role. The HCM object types that the job role accesses are identified automatically, and sections for the appropriate security profiles appear.

For example, if you select the job role human resource analyst, then sections for managed person, public person, organization, position, LDG, and document type appear. You select or create security profiles for those object types in the HCM data role.

If you select a job role that doesn't access any of the HCM objects that are secured by security profiles, then you can’t create an HCM data role.

Note

If you create custom job roles in Oracle Identity Management, then you must add them to a role category that ends with Job Roles. Otherwise, they don’t appear in the list of job roles when you create an HCM data role.

Security Profiles

For each object type, you can include only one security profile in an HCM data role.

Components of the HCM Data Role

The following figure summarizes the components of an HCM data role.

The job role that you select in the HCM data role inherits multiple duty roles. Each duty role has one or more function security privileges and related data security policies, from which the relevant HCM object types are identified.
automatically. The specific instances of the objects required by this HCM data role are identified in security profiles and stored in a data instance set.

For example, the human resource specialist job role inherits the employee hire and worker promotion duty roles, among many others. The duty roles provide both function security privileges, such as Hire Employee and Promote Workers, and access to objects, such as person and assignment. Security profiles identify specific instances of those objects for the HCM data role, such as people with assignments in a specified legal employer and department.

**HCM Security Profiles: Explained**

Security profiles identify instances of Human Capital Management (HCM) objects. For example, a person security profile identifies one or more person records, and a payroll security profile identifies one or more payrolls. This topic describes how to create and use security profiles and identifies the HCM objects that need them. To manage security profiles, you need the IT Security Manager job role.

**Use of HCM Security Profiles**

You include security profiles in HCM data roles to identify the data that users with those roles can access. You can also assign security profiles directly to abstract roles, such as employee. However, you’re unlikely to assign them directly to job roles, because users with same job role usually access different sets of data.

**HCM Object Types**

You can create security profiles for the following HCM object types:

- Person
- Managed person
- Public person
- Organization
Creating HCM Data Roles

- Position
- Legislative data group (LDG)
- Country
- Document type
- Payroll
- Payroll flow

Two uses exist for the person security profile because many users access two distinct sets of people.

- The Managed Person security profile identifies people you can perform actions against.
- The Public Person security profile identifies people you can search for in the worker directory.

This type of security profile also secures some lists of values. For example, the Change Manager and Hire pages include a person list of values that the public person security profile secures. The person who's selecting the manager for a worker may not have view access to that manager through a managed person security profile.

Security Criteria in HCM Security Profiles

In a security profile, you specify the criteria that identify data instances of the relevant type. For example, in an organization security profile, you can identify organizations by organization hierarchy, classification, or name. All criteria in a security profile apply. For example, if you identify organizations by both organization hierarchy and classification, then only organizations that satisfy both criteria belong to the data instance set.

Security Profile Creation

You can create security profiles either individually or while creating an HCM data role. For standard requirements, it's more efficient to create the security profiles individually and include them in appropriate HCM data roles.

To create security profiles individually, use the relevant security profile task. For example, to create a position security profile, use the task Manage Position Security Profiles (Navigator - Tools - Setup and Maintenance - Manage Position Security Profiles).

Security profiles that provide view-all access are predefined.

Reusability and Inheritance of Security Profiles

Regardless of how you create them, all security profiles are reusable. You can include security profiles in other security profiles. For example, you can include an organization security profile:

- In a person security profile, to secure person records by department, business unit, or legal employer
- In a position security profile, to secure positions by department or business unit

One security profile inherits the data instance set defined by another.

Predefined HCM Security Profiles: Explained

The Oracle Human Capital Management Cloud security reference implementation includes the following predefined HCM security profiles.
You can include the predefined security profiles in any HCM data role, but you can’t edit them. The View all option is disabled in any security profile that you create. This restriction exists because predefined security profiles meet this requirement.

Creating an HCM Data Role: Worked Example

This example shows how to create an HCM data role.

The legal employer ABC Industrial has sales, development, and manufacturing departments. This example shows how to create an HCM data role for a human resource (HR) specialist in the sales department.

The following table summarizes key decisions for this scenario.

<table>
<thead>
<tr>
<th>Decisions to Consider</th>
<th>In This Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s the name of the HCM data role?</td>
<td>HR Specialist ABC Industrial - Sales Department</td>
</tr>
</tbody>
</table>
Decisions to Consider | In This Example
--- | ---
Which job role does the HCM data role include? | Human Resource Specialist
Can the role be delegated? | Yes
Which person records do users access? | Users access the managed person records of:
- All workers in the sales department
- The emergency contacts, beneficiaries, and dependents of all workers in the sales department
Which public person records do users access? | All
Which organizations do users access? | All organizations of all types in ABC Industrial
Which positions do users access? | Vice President of Sales and all subordinate positions in the position hierarchy of ABC Industrial
Which countries do users access? | All
Which legislative data groups (LDGs) do users access? | The LDG for the legal employer ABC Industrial. An LDG security profile exists for this LDG.
Which document types do users access? | All
Which payrolls do users access? | Payrolls for the legal employer ABC Industrial. A payroll security profile exists for these payrolls.
Which payroll flows do users access? | Payroll flows for the legal employer ABC Industrial. A payroll flow security profile exists for these payroll flows.

**Summary of the Tasks**

Create the HCM data role by:
1. Naming the HCM data role and selecting the associated job role
2. Specifying the security criteria for each HCM object type
3. Creating security profiles
4. Reviewing and submitting the HCM data role

**Naming the HCM Data Role and Selecting the Job Role**

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 Results section of the Manage Data Roles and Security Profiles page, click Create.
4. On the Create Data Role: Select Role page, complete the fields as shown in this table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role</td>
<td>HR Specialist ABC Industrial - Sales Department</td>
</tr>
<tr>
<td>Job Role</td>
<td>Human Resource Specialist</td>
</tr>
<tr>
<td>Delegation Allowed</td>
<td>Yes</td>
</tr>
</tbody>
</table>

5. Click Next.

**Specifying Security Criteria for Each HCM Object Type**

1. In the Organization section of the Create Data Role: Security Criteria page, complete the fields as shown in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Security Profile</td>
<td>Create New</td>
</tr>
<tr>
<td>Name</td>
<td>ABC Industrial - All Organizations</td>
</tr>
<tr>
<td>Secure by organization hierarchy</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2. In the Position section, complete the fields as shown in the table

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Security Profile</td>
<td>Create New</td>
</tr>
<tr>
<td>Name</td>
<td>ABC Industrial Positions - Top Position Vice President of Sales</td>
</tr>
<tr>
<td>Secure by position hierarchy</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3. In the Countries section, select the predefined country security profile View All Countries.

4. In the Legislative Data Group section, select the existing LDG security profile ABC Industrial LDGs.

5. In the Person section, complete the fields as shown in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Security Profile</td>
<td>Create New</td>
</tr>
</tbody>
</table>
6. In the Public Person section, select the predefined person security profile View All People.

7. In the Document Type section, select the predefined document type security profile View All Document Types.

8. In the Payroll section, select the existing payroll security profile ABC Industrial Payrolls.

9. In the Payroll Flow section, select the existing payroll flow security profile ABC Industrial Payroll Flows.

10. Click **Next**.

**Creating the Organization Security Profile**

1. In the Organization Hierarchy section of the Assign Security Profiles to Role: Organization Security Profile page, select the **Secure by organization hierarchy** option.

2. Complete the fields in the Organization Hierarchy section as shown in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree Structure</td>
<td>Generic organization hierarchy</td>
</tr>
<tr>
<td>Organization Tree</td>
<td>ABC Industrial Organization Tree</td>
</tr>
<tr>
<td>Top Organization Selection</td>
<td>Use the assignment department</td>
</tr>
<tr>
<td>Include top organization</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3. Click **Next**.

**Creating the Position Security Profile**

1. In the Position Hierarchy section of the Assign Security Profiles to Role: Position Security Profile page, select the **Secure by position hierarchy** option.

2. Complete the fields in the Position Hierarchy section as shown in the table.
3. Open the Assign Security Profile to Role: Person Security Profile page.

Creating the Person Security Profile

1. In the Basic Details section of the Assign Security Profiles to Role: Person Security Profile page, select the Include related contacts option.

2. In the Person Types section, select the Secure by person type option, and complete the fields as shown in the table.

<table>
<thead>
<tr>
<th>Type</th>
<th>System Person Type</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Employee</td>
<td>Restricted</td>
</tr>
<tr>
<td>System</td>
<td>Contingent worker</td>
<td>Restricted</td>
</tr>
<tr>
<td>System</td>
<td>Nonworker</td>
<td>Restricted</td>
</tr>
<tr>
<td>System</td>
<td>Pending worker</td>
<td>Restricted</td>
</tr>
</tbody>
</table>

3. In the Workforce Structures section, select the Secure by department option. Select the existing organization security profile ABC Industrial - Sales Department.

4. Click Review.

Review and Submit the HCM Data Role

1. On the Create Data Role: Review page, review the HCM data role.

2. Click Submit.

3. On the Manage Data Roles and Security Profiles page, search for the HCM data role. In the search results, confirm that the role status is Requested. Once the role status is Request Complete, you can provision the role to users.
Creating HCM Data Roles and Security Profiles: Points to Consider

Planning your use of HCM data roles and security profiles enables you to minimize maintenance and ease the introduction of HCM data roles and security profiles in your enterprise. This topic suggests some approaches.

Identifying Standard Requirements

Most enterprises are likely to have some standard requirements for data access. For example, multiple HCM data roles may need access to all person records in a specific legal employer. If you create a person security profile that includes all person records in that legal employer, then you can include it in multiple HCM data roles. This approach simplifies the management of HCM data roles and security profiles, and may also prevent the creation of duplicate security profiles.

Naming HCM Data Roles and Security Profiles

You’re recommended to define and use a naming scheme for HCM data roles and security profiles.

A security profile name can identify the scope of the resulting data instance set. For example, the person security profile name All Employees Sales Department conveys that the security profile identifies all employees in the Sales Department.

An HCM data role name can include both the name of the inherited job role and the data scope. For example, the HCM data role Human Resource Analyst Finance Division identifies both the job role and the organization within which the role operates. HCM data role names must be less than 55 characters.

Planning Data Access for Each HCM Data Role

An HCM data role can include only one security profile of each type. For example, you can include one organization security profile, one managed person security profile, and one public person security profile. Therefore, you must plan the requirements of any HCM data role to ensure that each security profile identifies all required data instances. For example, if a user accesses legal employers and departments, then the organization security profile in the user’s HCM data role must identify both types of organizations.

Providing Access to All Instances of an Object

To provide access to all instances of an HCM object, use the appropriate predefined security profile. For example, to provide access to all person records in the enterprise, use the predefined security profile View All People.

Role Delegation: Explained

Role delegation is the assignment of a role from one user, known as the delegator, to another user, known as the proxy. The delegation can be either for a specified period, such as a planned absence, or indefinite.
You can delegate roles in the Roles and Approvals Delegated to Others section on the Manage User Account page. Select **Navigator - My Information - My Account**.

**Actions Enabled by Delegation**

The proxy user can perform the tasks of the delegated role on the relevant data. For example, a line manager can manage absence records for his or her reports. If that manager delegates the line manager role, then the proxy can also manage the absence records of the delegator’s reports. The delegator doesn't lose the role while it's delegated.

The proxy user signs in to Oracle Fusion HCM using his or her own user name, but has additional function and data privileges from the delegated role.

**Proxy Users**

You can delegate roles to any user whose details you can access by means of a public person security profile. This security profile typically controls access to person details in the person gallery.

**Roles That You Can Delegate**

You can delegate any role that you have currently, provided that:

- The role is enabled for delegation.
- The assignment that qualifies you for the role doesn't have a future-dated termination.

You can also delegate any role that you can provision to other users, provided that the role is enabled for delegation. By delegating roles rather than provisioning them to a user, you can:

- Specify a limited period for the delegation.
- Enable the proxy user to access your data.

**Duplicate Roles**

If the proxy user already has the role, then the role isn't provisioned again. However, the proxy user does gain access to the data that's accessible using the delegator’s role.

For example, you may delegate the line manager role to a proxy user who already has the role. The proxy user can access both your data (for example, the workers in your manager hierarchy) and his or her own data while the role is delegated.

The proxy’s My Account page shows the delegated role in the Roles Delegated to Me section, even though only the associated data has been delegated.

**Termination of Role Delegation**

If you enter an end date when delegating a role, then the delegation ends on that date. The Send Pending LDAP Requests process sends the request to end the role delegation to Oracle Identity Management on the specified end date.

You can enter or update an end date at any time during the delegation period. If the end date is today’s date, then the delegation ends immediately.
Role delegation ends before the specified end date if the proxy user's assignment is terminated.

**FAQs for HCM Data Roles and Security Profiles**

**What happens if I edit an HCM data role?**

You can edit or replace the security profiles in an HCM data role. Saving your changes updates the relevant data instance sets. Users with this HCM data role find the updated data instance sets when they next sign in.

You can’t change the HCM data role name or select a different job role. To make such changes, you create a new HCM data role and disable this HCM data role, if appropriate.

**How do I provision HCM data roles to users?**

On the Create Role Mapping page, create a role mapping for the role.

Select the **Autoprovision** option to provision the role automatically to any user whose assignment matches the mapping attributes.

Select the **Requestable** option if any user whose assignment matches the mapping attributes can provision the role manually to other users.

Select the **Self-Requestable** option if any user whose assignment matches the mapping attributes can request the role.

**What happens if I edit a security profile that's enabled?**

If the security profile is in use, saving your changes updates the security profile's data instance set. For example, if you remove a position from a position security profile, the position no longer appears in the data instance set. Users find the updated data instance set when they next access the data.

**What happens if I disable a security profile?**

The security profile returns no data. For example, a user with an HCM data role that allows the user to update organization definitions would continue to access organization-related tasks. However, the user couldn’t access organizations identified in a disabled organization security profile.

You can’t disable a security profile that another security profile includes.

**Person Security Profiles**

**Creating Person Security Profiles: Examples**

These examples show typical requirements for person security profiles. Use the Manage Person Security Profiles task in the Setup and Maintenance work area.
Human Resource Specialists for a Legal Employer

Human resource (HR) specialists for the ABC legal employer manage person records of workers who have a work relationship with ABC. You create a person security profile named All ABC Workers. You:

- Secure by person type and select the system person types employee, contingent worker, nonworker, and pending worker.
- Set the access level to Restricted for these person types.
- Secure by legal employer.
- Select an organization security profile that identifies legal employer ABC and any subordinate organizations.

Payroll Administrators for a Subset of Employees

Your enterprise has several payroll administrators in Ireland. Some manage employee records for names in the range A through M, and some manage those in the range N through Z. Therefore, you create two person security profiles, Employees A to M and Employees N to Z.

- In both security profiles, you
  - Secure by person type, select the employee system person type, and set the access level to Restricted.
  - Secure by legal employer and select an organization security profile that identifies legal employers in Ireland.
  - In the security profile Ireland Employees A to M, you secure by global name range and set the range to A through M.
  - In the security profile Ireland Employees N to Z, you secure by global name range and set the range to N through Z.

Securing Person Records by Manager Hierarchy: Points to Consider

The person records that a manager can access depend on how you specify the manager hierarchy in the person security profile. This topic describes the available options. To create a person security profile, use the Manage Person Security Profile or Manage Data Role and Security Profiles task. You can access both tasks in the Setup and Maintenance work area (Navigator - Tools - Setup and Maintenance).

For the manager hierarchy, you can select one of:

- Person-level manager hierarchy
- Assignment-level manager hierarchy

The manager-hierarchy value always controls access to person records, including all assignments. You can't enable access to particular assignments.

Note
Managers other than line managers can access person records secured by manager hierarchy only if their roles have the appropriate access to functions and data. Providing this access is a security-customization task.

Consider the following example manager hierarchy.

Harry is a line manager with two assignments. In his primary assignment, he manages Sven’s primary assignment. In his assignment 2, Harry manages Jane’s primary assignment. Monica is a line manager with one assignment. She manages Jane’s assignment 2 and Amir’s primary assignment. In her primary assignment, Jane manages Franco’s primary assignment. In her assignment 2, Jane manages Kyle’s primary assignment.

**Person-Level Manager Hierarchy**

The security profile’s data instance set includes any person in a direct or indirect reporting line to any of the signed-in manager’s assignments.

In this scenario, Harry accesses the person records for Sven, Jane, Franco, and Kyle.

Monica accesses the person records for Jane, Franco, Kyle, and Amir.
Jane accesses the person records for Franco and Kyle.

Using the person-level hierarchy, the signed-in manager accesses the person records of every person in his or her manager hierarchy, subject to any other criteria in the security profile.

**Assignment-Level Manager Hierarchy**

Managers see the person records of people who:

- Report to them directly from one or more assignments
- Report to assignments that they manage

In this scenario, Harry accesses person records for Sven, Jane, and Franco. He can't access Kyle's record, because Kyle reports to an assignment that Monica manages.

Monica accesses person records for Jane, Kyle, and Amir. She can't access Franco's record, because Franco reports to an assignment that Harry manages.
Jane accesses person records for Franco and Kyle.

An assignment-level manager hierarchy isn’t the same as assignment-level security, which would secure access to individual assignments. You can’t secure access to individual assignments.

**Specifying the Manager Type: Explained**

When you secure person records by manager hierarchy, the security profile’s data instance set comprises person records from manager hierarchies of the specified types. This topic describes the available type values and explains their effects. You select a **Manager Type** value when you perform the Manage Person Security Profile task.

The following table describes the **Manager Type** values.

<table>
<thead>
<tr>
<th>Manager Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>The security profile includes all types of manager hierarchies.</td>
</tr>
<tr>
<td>Line Manager</td>
<td>The security profile includes only the line manager hierarchy.</td>
</tr>
<tr>
<td>Selected</td>
<td>The security profile includes only the specified type of manager hierarchy.</td>
</tr>
</tbody>
</table>

Typically, you select **Line Manager** for line managers, **Project Manager** for project managers, and so on. If you select **All**, then users with the line
manager job role (for example) have line-manager access to all of their manager hierarchies. Avoid selecting All if this level of access isn't required.

Manager Job Roles

Manager job roles other than line manager aren't predefined. Creating job roles for managers such as project managers and resource managers is a security-customization task. Once those roles exist, you can assign security profiles to them (either directly or by creating a separate HCM data role). Users with those roles can then access their manager hierarchies in the Manager Resources dashboard and elsewhere.

Hierarchy Content: Explained

The Hierarchy Content attribute controls how access to manager hierarchies is delegated when you:

- Secure access to person records by manager hierarchy.
- Delegate a role that includes the person security profile.

Create person security profiles on the Create Person Security Profile page. Select Navigator - Tools - Setup and Maintenance and search for the Manage Person Security Profile task.

Hierarchy Content Values

This table describes the Hierarchy Content values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager hierarchy</td>
<td>The manager hierarchy of the signed-in user. This value is the default value. Don't use this value if the associated role can be delegated.</td>
</tr>
<tr>
<td>Delegating manager hierarchy</td>
<td>The manager hierarchy of the delegating manager. Select this value if the associated role is always delegated to a user who isn't a manager and therefore has no manager hierarchy.</td>
</tr>
<tr>
<td>Both</td>
<td>The proxy user can access both his or her own manager hierarchy and the hierarchy of the delegating manager. Select this value for the typical case of one manager delegating a line manager role to another manager.</td>
</tr>
</tbody>
</table>

When a user delegates a line manager role to another line manager, the proxy user can manage the delegator's reports in the Person Management work area and person gallery. However, the proxy's Manager Resources dashboard doesn't show the delegator's reports because the manager hierarchy isn't changed by the role delegation.
Note
If the proxy user is in the delegator's manager hierarchy, then the delegated role gives the proxy user access to his or her own record.

Securing Person Records by Workforce Structures: Points to Consider

In a person security profile, you can identify person records by one or more work structures. Available work structures are department, business unit, legal employer, position, payroll, and legislative data group (LDG). This topic explains the effect of each of these values on the security profile's data instance set. You select workforce structures when you perform the Manage Person Security Profile task.

Identifying the Work Structures

You identify each work structure using a security profile of the relevant type. This table shows the security profile type for each work structure.

<table>
<thead>
<tr>
<th>Work Structure</th>
<th>Security Profile Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Organization</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Organization</td>
</tr>
<tr>
<td>Legal Employer</td>
<td>Organization</td>
</tr>
<tr>
<td>Position</td>
<td>Position</td>
</tr>
<tr>
<td>LDG</td>
<td>Legislative Data Group</td>
</tr>
<tr>
<td>Payroll</td>
<td>Payroll</td>
</tr>
</tbody>
</table>

These security profiles are reusable. You can include them in any person security profile to identify a set of person records. The person security profile inherits the data instance set of any security profile that you include.

Using Assignment-Level Attributes

Although the department, business unit, payroll, and position values are assignment attributes, you can’t secure access to individual assignments. If one of a person’s assignments satisfies the criteria in a person security profile, all of the person’s assignments belong to the data instance set.

Securing Person Records by LDG

The LDG must be associated with the payroll statutory unit of the person’s legal employer. In this case, the security profile’s data instance set includes the person’s record and all assignments.
Securing Person Records by Payroll

A person’s record and all assignments belong to the security profile’s data instance set if at least one of the person’s assignments includes the payroll.

Securing Person Records by Legal Employer

Workers with at least one work relationship of any type with the specified legal employer belong to the security profile’s data instance set. Any assignments that these workers have, in work relationships of any type with any legal employer, belong to the data instance set.

Other criteria in the person security profile may limit the effects of securing by legal employer. For example, only persons with employee work relationships with the legal employer belong to the security profile’s data instance set if you also:

• Secure person records by person type.
• Select the Employee system person type.
• Set Access to Restricted.

The security profile’s data instance set excludes person records for other person types.

Securing Person Records Using Custom Criteria: Examples

You can secure person records by person type, manager hierarchy, workforce structures, and global name range. You can also specify custom criteria, in the form of SQL statements, in addition to or in place of the standard criteria. This topic shows how to specify custom criteria in a person security profile when you perform the Manage Person Security Profile task.

The custom criteria can include any statement where the predicate restricts by PERSON_ID or ASSIGNMENT_ID. The custom predicate must include either &TABLE_ALIAS.PERSON_ID or &TABLE_ALIAS.ASSIGNMENT_ID as a restricting column in the custom criteria.

This scenario shows how to use custom criteria in a person security profile.

Identifying Persons Born Before a Specified Date

The person security profile data instance set must include employees in a single legal employer who were born before 01 January, 1990. You secure person records by:

• Person type. You select the Employee system person type and set the access level to Restricted.
• Legal employer. You select an organization security profile that identifies the relevant legal employer and its subordinate organizations.

You also secure by custom criteria, and enter the following statement:

&TABLE_ALIAS.PERSON_ID IN (SELECT PERSON_ID FROM PER_PERSONS
FAQs for Person Security Profiles

Can users access the contact records of the people they can access?

Not automatically. However, you can include a person’s contacts in the person security profile's data instance set by selecting the security profile option Include related contacts.

Note

If a person’s contact is also a worker, then the contact’s person record appears in the data instance set only if it matches all criteria in the security profile.

What happens if a person has multiple assignments or person types?

A user who can access a person record can access all of the person’s assignments. For example, a user who can access employee records in a particular legal employer can access all of their assignments, even if some are contingent worker or nonworker assignments with different legal employers.

What happens if a person has no assignments?

Person records without assignments, such as those of emergency contacts, don’t have to satisfy any assignment criteria in the person security profile. They need to satisfy only the person-related criteria (person type, global name range, and custom criteria). Such records are an exception to the rule that all security profile criteria must be satisfied.

What happens if I select an organization security profile for a generic organization hierarchy?

If you secure by department, for example, the data instance set includes only organizations with the department classification from the generic organization hierarchy. The data instance set excludes other types of organizations. Therefore, you can select the same organization security profile for multiple work structure types.

What happens if I use the department or position from the user’s assignment as the top department or position?

The user’s access to the organization or position hierarchy depends on the user’s assignments. Therefore, the data instance set from a single security profile may be different for each user.

For a user with multiple assignments in the hierarchy, multiple top organizations or positions may exist. All organizations or positions from the relevant subhierarchies appear in the data instance set.
Creating Organization Security Profiles: Examples

An organization security profile identifies organizations by at least one of organization hierarchy, organization classification, and organization list. These examples show some typical requirements for organization security profiles. Use the Manage Organization Security Profile task to create organization security profiles.

HR IT Administrator Who Maintains Organizations

The HR IT administrator maintains all types of organizations for the enterprise. The user’s access must reflect any changes to the organization hierarchy without requiring updates to the security profile. Therefore, you:

- Secure by organization hierarchy.
- Select a generic organization hierarchy. The security profile includes organizations of all classifications.
- Identify by name the top organization in the hierarchy. The top organization is unlikely to vary with the user’s own assignments.

If you secure by organization classification or list organizations by name, then you must maintain the security profile as the organization hierarchy evolves.

Human Resource Specialist Who Manages Employment Records in a Legal Employer

The human resource (HR) specialist accesses lists of various organizations, such as legal employers and business units, while managing employment information. To identify the organizations that the user can see in such lists, you:

- Secure by organization hierarchy.
- Select a generic organization hierarchy, because the user accesses more than one type of organization.
- Use the department from the user’s assignment as the top organization in the hierarchy. Using this value means that you can assign an HCM data role that includes this organization security profile to multiple HR specialists.

The HR specialist also needs access to person records, which you can secure by organization. If the set of organizations is the same, then you can reuse this organization security profile to secure the person records in a person security profile.

Securing Organizations: Points to Consider

Some users maintain organization definitions. Others access lists of organizations while performing tasks such as creating assignments. The access requirements for these users differ. However, for both types of users you identify
relevant organizations in an organization security profile. This topic discusses the effects of options that you select when creating an organization security profile. To create an organization security profile, use the Manage Organization Security Profile task.

**Organizations with Multiple Classifications**

Organizations may have more than one classification. For example, a department may also have the legal employer classification. An organization belongs to an organization security profile data instance set if it satisfies any one of the security profile's classification criteria. For example, if you secure by department hierarchy only, a department that's also a legal employer is included because it's a department.

**Selecting the Top Organization in an Organization Hierarchy**

If you select a named organization as the top organization in an organization hierarchy, then you must ensure that the organization remains valid. No automatic validation of the organization occurs, because changes to the organization hierarchy occur independently of the organization security profile.

**Users With Multiple Assignments**

You can select the department from the user's assignment as the top organization in an organization hierarchy. Multiple top organizations may exist if the user has multiple assignments. In this case, all organizations from the relevant subhierarchies of the organization hierarchy belong to the organization security profile data instance set.

The following figure illustrates the effects of this option when the user has multiple assignments.

The user has two assignments, one in organization B and one in organization D, which belong to the same organization hierarchy. The top organizations are organizations B and D, and the user's data instance set of organizations therefore includes organizations B, E, D, F, and G.
Creating Position Security Profiles: Examples

These scenarios show typical uses of position security profiles. To create a position security profile, use the Manage Position Security Profile task.

Human Resource Specialist Who Manages Position Definitions
The human resource (HR) specialist manages most position definitions for the enterprise. To identify the positions, you:

- Secure by position hierarchy. You select the enterprise position hierarchy tree, identify the top position, and include it in the hierarchy.
- Secure by position list. You exclude by name any positions for which the HR specialist isn’t responsible.

You can include this security profile in an HCM data role and provision the role to any HR specialist who’s responsible for these position definitions.

Line Manager Who Hires Workers
Line managers in your business unit can hire workers whose positions are below the managers’ own positions in the position hierarchy. To identify these positions, you:

- Secure by position hierarchy, and select the position tree.
- Use the position from the user’s assignment as the top position.
  You don’t include the top position in the hierarchy.

You can include this position security profile in an HCM data role and provision the role to any line manager in your business unit.

Person Records Secured by Position
Some senior managers in your enterprise can access the person records of workers below them in the position hierarchy. Therefore, you secure access to those person records by position in the person security profile. To identify the positions, you create a position security profile where you:

- Secure by position hierarchy, and select the position tree.
- Identify the senior manager position as the top position, but don’t include it in the hierarchy.
  This exclusion ensures that senior managers can’t access the person records of other senior managers.

Creating Document Type Security Profiles: Examples

Some users manage document types for the enterprise. Others manage documents associated with the person records that they access. For example, workers manage their own documents. For all access requirements, you identify the document types that users can access in a document type security profile. These scenarios show typical uses of document type security profiles. To create a document type security profile, use the Manage Document Type Security Profile task.
Note
Document type security profiles secure access to custom document types only. They don’t secure access to standard predefined document types, such as visas, work permits, and driver’s licenses. Access to person records provides access to the standard predefined document types.

Workers Managing Their Own Documents
Workers can manage their own documents from their portraits. Implementors typically assign the predefined security profile View All Document Types directly to the employee and contingent worker roles. Workers can therefore access their own documents.

Alternatively, you can create a document type security profile that includes specified document types only. In the security profile, you list document types to either include or exclude. For example, you could create a document type security profile for workers that excludes disciplinary or medical documents. Workers would access all other document types.

Human Resource Specialists Managing Document Types
Human resource (HR) specialists who manage the enterprise document types must access all document types. You can provide this access by including the predefined security profile View All Document Types in the HCM data role that you provision to HR specialists. Using this security profile, HR specialists can also manage custom documents in the person records that they manage.

Legislative Data Group Security Profiles: Explained

You use a legislative data group (LDG) security profile to identify one or more LDGs to which you want to secure access. Use the Manage Legislative Data Group Security Profiles task in the Setup and Maintenance work area (Navigator - Tools - Setup and Maintenance).

View All Legislative Data Groups Security Profile
The predefined LDG security profile View All Legislative Data Groups provides access to all enterprise LDGs. Use this security profile wherever appropriate. For example, if users with a particular HCM data role manage all enterprise LDGs, then include View All Legislative Data Groups in that data role.

Custom LDG Security Profiles
If responsibility for particular LDGs belongs to various HCM data roles, then you create an appropriate LDG security profile for each data role. For example, you may need one LDG security profile for European LDGs and one for American LDGs.

Access to Person Records
You can use an LDG security profile to secure access to person records. The LDG must be associated with the payroll statutory unit of a person’s legal employer. In this case, the person’s record belongs to the person security profile data instance set.
Creating Payroll Security Profiles: Examples

These examples illustrate different methods by which access to payrolls can be assigned to members of the Payroll department. Payroll definitions are first organized into appropriate payroll security profiles through the Manage Payroll Security Profiles task. The security profile is then included in an HCM data role or assigned directly to a job role, and that role is provisioned to a user.

**Payroll Period Type**
This example illustrates the most common scenario, where payrolls are organized by their period type. Monthly payrolls are sorted into the same security profile; semiweekly into another; and so on. The security profile is then included in an HCM data role or assigned directly to a job role, and that role is provisioned to the payroll administrators.

**Regional Assignments**
This example illustrates the scenario where payrolls are organized by the regions of the target employees’ work areas. For example, payrolls run against North American facilities are added to one security profile, while European facilities are added to another.

**Individual Contributors**
This example illustrates an ad hoc implementation where payrolls are organized according to the work responsibilities of the owning Payroll Manager. For example, payroll access may be restricted only to those administrators who created and manage their definitions.

Creating Payroll Flow Security Profiles: Examples

The following examples illustrate different methods by which payroll flows can be organized into appropriate security profiles. Access to those profiles is granted to workers through the Assign Security Profiles to Role page. Users must also be granted access to the appropriate tasks within the flow.

**Payroll Processing and QuickPay Flows**
Payroll administrators responsible for payroll processing would be granted permission to submit the Payroll Cycle and QuickPay flows. Therefore, their payroll flow security profiles must include the appropriate flows.

**End of Year Reporting**
Administrators responsible for End of Year reporting would be granted permission to submit the End of Year and Archive End-of-Year Payroll Results flows. Therefore, their payroll flow security profiles must include the appropriate flows.

**Hiring and Terminations**
Administrators responsible for hiring and terminations should be granted permission to flows such as New Hire flow and Termination flow.
Payroll Flow Security and Flow Owners: Explained

Your HCM data role security determines which payroll flows you can submit or view on the Payroll Dashboard or payroll work areas, including flows delivered for a single report or process. When you submit a payroll flow, you become the payroll flow checklist owner.

Payroll Checklist Owners and Task Owners

The payroll checklist owner inherits any task within the flow, unless the payroll flow pattern specifies a different owner for a task. A checklist or task owner can reassign a task to someone else. For example, as a checklist owner, if a task is overdue and the task owner is on leave, you might reassign the task to another team member.

Payroll Flow Security and HCM Data Roles

HCM data roles secure the access to payroll flows through data privileges and to the payroll tasks on a payroll checklist through functional privileges. If you cannot:

- Submit or view a payroll flow, confirm that the data role assigned to you includes a security profile for the payroll flow pattern.
- Perform a task such as a process or report, confirm that your data role is based on a job or abstract role whose inherited duty roles include necessary functional privilege to perform that task.

In the following figure, both the payroll administrator and the payroll manager are assigned duty roles with the functional privilege to submit a process or report and the data privilege to view the data for the monthly payroll flow pattern. Both the manager and administrator can perform the same task or have that task reassigned to them.
In the following figure, only the payroll manager not the payroll administrator job role inherits the functional privilege to calculate payroll. The payroll manager should not reassign a flow task to a payroll administrator, because the administrator does not have the necessary functional privilege.

FAQs for Organization and Other Security Profiles

What’s the difference between a generic organization hierarchy and a department hierarchy?

A generic organization hierarchy is a single hierarchy that includes organizations of all classifications, such as division, legal entity, department, and tax reporting unit.

A department hierarchy includes only organizations with the department classification.

When do I need a country security profile?

Country security profiles identify one or more countries to appear in lists of countries. The predefined country security profile View All Countries meets most needs. However, you can limit the country list available to an HCM data role by creating a country security profile for that role. The countries that you can include are those defined in the table FND_TERRITORIES.
Managing HCM Data Roles

Minimizing the Number of Data Roles: Explained

If you create data roles for specific data instance sets, then the number of data roles in the enterprise may grow quickly. This growth can make maintaining data roles difficult. You're recommended to plan your use of data roles and minimize their number by using dynamic security profiles wherever possible.

For example, Tom, Jorge, and Linda are all human resource specialists (HR specialists) for employees in different business units. Each has a data role that inherits the Human Resource Specialist job role because they all perform the same job. However, they access different sets of data. You could create four different data roles, each with its own static security profile, as shown here:

In this example, access to person and assignment data is secured by business unit (BU). However, you could base it on legal employer or department, for example.

Areas of Responsibility and Dynamic Security Profiles

As an alternative to using static security profiles, you could:

- Define an area of responsibility for each HR specialist using the Manage Areas of Responsibility task. Select **Navigator - Workforce Management - Person Management - Manage Areas of Responsibility**.

  In each case, the scope of responsibility would be the relevant business unit. For example, Tom’s area of responsibility would be USA1 BU. Jorge would have two areas of responsibility, one for USA2 BU and one for USA Health BU.

- Create a person security profile that restricts access based on the defined areas of responsibility.
In the Custom Criteria section, you enter a SQL fragment that grants each HR specialist access to person records based on areas of responsibility.

Using this approach, you need just two data roles:

- **User: Tom Green**
- **User: Jorge Blum**
- **User: Linda Swift**

**Minimizing the Number of Data Roles: Examples**

This example summarizes how to:

- Create an area of responsibility for a user.
- Create a person security profile with custom criteria that use areas of responsibility to define data security.

**Creating an Area of Responsibility**

Use the Manage Areas of Responsibility task. Select **Navigator - Workforce Management - Person Management**.

Complete the Create Area of Responsibility page as shown in this table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility Name</td>
<td>USA1 BU Area</td>
</tr>
<tr>
<td>Responsibility Type</td>
<td>Human resources representative</td>
</tr>
<tr>
<td>From Date</td>
<td>First day of the current month</td>
</tr>
<tr>
<td>Business Unit</td>
<td>USA1 Business Unit</td>
</tr>
</tbody>
</table>

**Creating the Person Security Profile**

Sign in as the IT Security Manager.

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 Person Security Profile task.

The Manage Person Security Profiles page opens.

3. In the Search Results section, click Create.

The Create Person Security Profile page opens.

4. In the Name field, enter Access by Areas of Responsibility.

5. In the Custom Criteria section, select Secure by Custom Criteria. Enter the following SQL fragment in the text box:

```sql
EXISTS
(SELECT 1 FROM PER_ALL_ASSIGNMENTS_M A
WHERE A.ASSIGNMENT_TYPE IN ('E', 'C', 'N', 'P')
AND A.EFFECTIVE_LATEST_CHANGE='Y'
AND TRUNC(SYSDATE) BETWEEN LEAST(TRUNC(SYSDATE), A.EFFECTIVE_START_DATE) AND A.EFFECTIVE_END_DATE
AND A.PERSON_ID=&TABLE_ALIAS.PERSON_ID
AND EXISTS
(SELECT 1
FROM PER_ASG_RESPONSIBILITIES B,
PER_USERS C
WHERE A.BUSINESS_UNIT_ID=B.BUSINESS_UNIT_ID
AND C.USER_GUID=FND_GLOBAL.USER_GUID
AND C.PERSON_ID=B.PERSON_ID
AND B.RESPONSIBILITY_TYPE='HR_REP'
AND trunc(sysdate) between B.START_DATE and nvl(B.END_DATE,sysdate)))
```

This fragment restricts access to persons based on the:

- Responsibility type
- Business unit
- Area of responsibility from date
- Effective dates of the worker’s assignment

You can now select this security profile in relevant data roles.

**HCM Data Roles Configuration Diagnostic Test**

The HCM Data Roles Configuration diagnostic test verifies that the Manage HCM Data Roles task flow is configured successfully for a specified user.

To run the HCM Data Roles Configuration diagnostic test, select Settings and Actions - Troubleshooting - Run Diagnostic Tests.

**Diagnostic Test Parameters**

User Name
The test is performed for the specified user. The user doesn’t have to be signed-in while the test is running. However, the user must have signed in at least once, because the test uses details from the user’s current or latest session.

**HCM Security Profile Configuration Diagnostic Test**

The HCM Security Profile Configuration diagnostic test verifies that the Manage Security Profiles task flows are configured successfully for a specified user.

To run the HCM Security Profile Configuration diagnostic test, select **Settings and Actions - Troubleshooting - Run Diagnostic Tests**.

**Diagnostic Test Parameters**

**User Name**

The test is performed for the specified user. The user doesn’t have to be signed-in while the test is running. However, the user must have signed in at least once, because the test uses details from the user’s current or latest session.

**HCM Securing Objects Metadata Diagnostic Test**

The HCM Securing Objects Metadata diagnostic test validates securing-object metadata for the HCM securing objects.

To run the HCM Securing Objects Metadata diagnostic test, select **Settings and Actions - Troubleshooting - Run Diagnostic Tests**.

**Diagnostic Test Parameters**

**Securing Object**

Enter the name of an HCM securing object from the following table.

<table>
<thead>
<tr>
<th>Securing Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSON</td>
<td>Person</td>
</tr>
<tr>
<td>LDG</td>
<td>Legislative data group</td>
</tr>
<tr>
<td>POSITION</td>
<td>Position</td>
</tr>
<tr>
<td>ORGANIZATION</td>
<td>Organization</td>
</tr>
<tr>
<td>PAYROLL</td>
<td>Payroll</td>
</tr>
<tr>
<td>FLOWPATTERN</td>
<td>Payroll flow</td>
</tr>
<tr>
<td>DOR</td>
<td>Document type</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>Country</td>
</tr>
</tbody>
</table>
If you don’t enter the name of a securing object, then the test applies to all securing objects.

**How can I diagnose any issues with HCM data roles and security profiles?**

Run these diagnostic tests by selecting **Settings and Actions - Troubleshooting - Run Diagnostic Tests**.

<table>
<thead>
<tr>
<th>Diagnostic Test Name</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCM Data Roles Configuration</td>
<td>Configuration of Manage HCM Data Roles for a user</td>
</tr>
<tr>
<td>HCM Data Role Detailed Information</td>
<td>Potential problems with a data role</td>
</tr>
<tr>
<td>HCM Security Profile Configuration</td>
<td>Configuration of Manage Security Profiles tasks for a user</td>
</tr>
<tr>
<td>HCM Security Profiles Detailed Information</td>
<td>Potential problems with security profiles of a type</td>
</tr>
<tr>
<td>HCM Securing Objects Metadata</td>
<td>Securing-object metadata</td>
</tr>
</tbody>
</table>
Security Terminology: Explained

Oracle Identity Management (OIM) is the identity store and Authorization Policy Manager (APM) is the policy store for Oracle Fusion Applications. OIM and APM are available independently and each has its own terminology. The terminology that Oracle Fusion Applications uses isn’t always the same as the terminology that OIM and APM use.

You must understand these terminology differences as you manage business objects in each product interface. This table shows the terminology that each product uses when referring to common business objects.

<table>
<thead>
<tr>
<th>Oracle Fusion Applications</th>
<th>Oracle Identity Management</th>
<th>Authorization Policy Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Job Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Abstract Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Duty Role</td>
<td></td>
<td>Application Role</td>
</tr>
<tr>
<td>Function Security Privilege</td>
<td></td>
<td>Entitlement</td>
</tr>
<tr>
<td>Secured Code Artifact (for example, a service, task flow, or batch program)</td>
<td></td>
<td>Resource</td>
</tr>
<tr>
<td>Database Table</td>
<td></td>
<td>Database Resource</td>
</tr>
<tr>
<td>Data Security Privilege</td>
<td></td>
<td>Action</td>
</tr>
</tbody>
</table>

OIM also refers to data, job, and abstract roles as enterprise roles.

Tip
APM refers to duty roles as application roles because they're specific to a particular grouping of applications, such as Oracle Fusion Human Capital Management.

---

### Reviewing Roles and Role Assignments in Oracle Identity Manager: Procedure

You use Oracle Identity Manager (OIM) to manage HCM job roles.

This procedure explains how to use OIM to:

- View the roles assigned to a user.
- List users who have a specific role.

#### Viewing the Roles Assigned to a User in Oracle Identity Manager

Sign in to Oracle Fusion Human Capital Management (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 Job Roles task.
   
   The Oracle Identity Manager - Self Service page opens.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click the **Administration** link in the top-right corner.
   
   The Oracle Identity Manager - Delegated Administration page opens.
4. On the Welcome tab of the Oracle Identity Manager - Delegated Administration page, click **Advanced Search - Users**. In the **Display Name** field, enter a user's display name (for example, John Smith) and select this user's name in the search results.
   
   A user page opens for this user.
5. Click the Roles tab to view the roles assigned to the user. This page shows all data, abstract, and job roles (if any) assigned to this user.
6. Return to the Welcome tab on the Oracle Identity Manager - Delegated Administration page.

#### Listing Users Who Have a Specific Role in Oracle Identity Manager

Follow these steps:

1. On the Welcome tab of the Oracle Identity Manager - Delegated Administration page, click **Advanced Search - Roles**.
2. Search for a role, for example, the Payroll Manager job role, and open it.
The role page opens.

**Tip**
The Attributes tab of the role page shows the role category name, such as HCM - Job Roles. This value identifies both the role type and the Oracle Fusion application where the role is used.

3. Click the Members tab.

On this tab, you can see all users who currently have the selected role.

**Tip**
On this tab, the Member Type is typically Indirect Role because you don’t usually assign job roles directly to users. Instead, they inherit them from data roles.

4. Click the Overview - Setup and Maintenance tab to return to Oracle Fusion HCM.

### Reviewing the Duties of a Predefined Job Role: Procedure

To review the duties of a predefined job role, you perform the Manage Duties task, as described in this topic.

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

1. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area and search for the Manage Duties task.

2. In the Search Results section, click Go to Task for the Manage Duties task.

   This action opens the Authorization Management page of Oracle Authorization Policy Manager (APM).

3. In the Application Name section on the APM Home tab, select hcm.

4. In the Search and Create section, click Search - External Roles. The Search - External Roles page opens.

**Tip**
Job roles, data roles, and abstract roles are all known as external roles in APM.

5. In the Display Name field, enter the name of the job role. For example, enter Benefits Administrator.

   Click Search.

6. Select the job role in the Search Results and click Open Role.

7. On the job role page, click the Application Role Mapping tab and open the hcm folder.
In the hcm folder you can see all of the duty roles that the selected job role inherits.

8. When your review is complete, click the Overview - Setup and Maintenance tab to return to the Setup and Maintenance work area.
Creating Custom Job or Abstract Roles

Creating a Custom Job or Abstract Role: Explained

If the predefined job or abstract roles don’t meet enterprise requirements, then you can create job or abstract roles. For example, you may want to create a job role because the duty roles that a predefined job role inherits aren’t as required. This topic introduces the three stages of creating a custom role. The stages are:

1. Create the custom job or abstract role in Oracle Identity Management (OIM) using the Manage Job Roles task.
2. Add duty roles to your custom role in Authorization Policy Manager (APM) using the Manage Duties task.

This process makes your custom role available in Oracle Fusion HCM. You can’t select the role in Oracle Fusion HCM interfaces until this process completes successfully. If you prefer, you can run it before you add duty roles to your custom role in APM.

Creating a Custom Job or Abstract Role: Procedure

Creating a custom job role or abstract role is a three-step process. This topic describes the first step, which is creating the custom role in Oracle Identity Management using the Manage Job Roles task.

Creating a Job or Abstract Role

Sign 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 Job Roles task. The Oracle Identity Manager Self-Service page opens.

3. On the Welcome tab of the Oracle Identity Manager Self-Service page, click Administration in the top-right corner. The Oracle Identity Manager - Delegated Administration page opens.

4. In the Roles section of the Welcome tab on the Oracle Identity Manager - Delegated Administration page, click Create Role.

5. In the Name field of the Create Role page, enter the name of your custom role. For example, enter SALES_DEPT_ADMIN_JOB.

6. In the Display Name field, enter the display name of your custom role. For example, enter Sales Department Administration Job Role.

7. In the Role Category Name field, search for and select either HCM - Job Roles or HCM - Abstract Roles, as appropriate.

8. Click Save.

Close the Oracle Identity Manager Delegated Administration Console tab to return to the Oracle Fusion Applications Setup and Maintenance work area.

Next steps of the process are:

1. Add duty roles to your custom job or abstract role.
2. Run the Retrieve Latest LDAP Changes process.

Adding Duties to a Job or Abstract Role : Procedure

This topic describes how to add duty roles to and remove them from a job or abstract role. If you create a custom job or abstract role, then you must follow this procedure to complete the role definition. This procedure is the second step in the three-step process to create a custom job or abstract role.

Adding Duty Roles to a Job or Abstract Role

Sign 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. The Oracle Entitlements Server Authorization Management page opens.

3. 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.
4. In the Search and Create section, click **Search - External Roles**.

5. In the Display Name field of the Search - External Roles page, search for the job or abstract role to which you're adding duty roles. For example, search for the job role Sales Department Administration Job Role.

6. In the Search Results section, select the role and click **Open Role**.

7. On the role page, click the Application Role Mapping tab.

8. Click **Map**.

   The **Map Application Roles to External Role** dialog box opens.

   a. In the **Application** field, select hcm.

   b. In the Display Name field, enter the name of the duty role that you want to add. For example, enter Department Management Duty.

   c. Click **Search**.

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

---

**Tip**

The selected duty role appears under the hcm folder on the Application Role Mapping tab of the role page. You can also delete duty roles on this tab.

---

Repeat step 8 for additional duty roles.

All application roles (duty roles) that you added now appear in the hcm folder on the Application Role Mapping tab.

Close the Oracle Entitlements Server: Authorization Policy Manager tab to return to the Oracle Fusion Applications Setup and Maintenance work area.

---

**Running Retrieve Latest LDAP Changes : Procedure**

---

After creating a custom job role or abstract role in Oracle Identity Management (OIM), you must run the Retrieve Latest LDAP Changes process. This process makes the role available to Oracle Fusion Human Capital Management (HCM). This topic describes how to run Retrieve Latest LDAP Changes.

---

**Note**

Once implementation is complete, you're recommended to schedule Retrieve Latest LDAP Changes to run daily. Once the process is scheduled, you can't run it on an as-needed basis.

If the process is scheduled when you create a custom job or abstract role, then you can wait for the process to complete its daily run. Once that run completes, the custom role is available in Oracle Fusion HCM. Alternatively, if you can't wait for the daily process, then you can end the scheduling temporarily and run the process as described here. When the process completes, you can schedule it again.
Running Retrieve Latest LDAP Changes

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

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
   
   The **Schedule New Process** dialog box opens.
3. In the **Name** field, search for and select the Retrieve Latest LDAP Changes process.
4. Click **OK** to close the **Schedule New Process** dialog box.
5. In the **Process Details** dialog box, click **Submit**.
6. Click **OK**, then **Close**.
7. On the Scheduled Processes page, click **Refresh**.
   
   Repeat this step periodically until the process completes.

Once the process completes successfully, you can select your custom role in Oracle Fusion HCM interfaces, such as Manage Data Roles and Security Profiles.

Creating Custom Duty Roles

Creating Custom Duty Roles: Procedure

Duty roles are made up of function security privileges and data security policies. You can create custom duty roles if the predefined duty roles don't meet your needs. For example, a predefined duty role may have more or fewer function security privileges or data security policies than you need. This topic shows how to create a custom duty role.

Once the duty role exists, you:

1. Add function security privileges to the duty role.
2. Add data security policies to the duty role.
3. Verify the duty role.

Creating a Duty Role

Sign 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. 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.
2. In the Application Name section of the Home tab, select **hcm**.
3. Under the Application Roles heading on the Home tab, select **New**.

An Untitled tab opens.

4. In the **Display Name** field on the Untitled tab, enter the display name of the new duty role. For example, enter Sales Department Management Duty.

5. In the **Role Name** field, enter the duty role name. For example, enter SALES_DEPT_MANAGE_DUTY.

6. Click **Save**.

The duty role's display name now appears as the tab name.

The next step is to add function security privileges to the duty role.

**Adding Function Security Privileges to a Duty Role : Procedure**

This topic explains how to create a security policy for a custom duty role and add an existing function security privilege to it. Typically, you perform this task immediately after creating a custom duty role.

**Adding Function Security Privileges to a Duty Role**

If you have just created a duty role and the duty role tab is still open, then:

- Select **Create Policy - Default Policy Domain** in the top-right corner of the tab to open an Untitled tab.

- Continue from step 5.

Otherwise, sign 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. 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.

2. In the **Application Name** section of the Home tab, select **hcm**. Under the Application Roles heading on the Home tab, click **Search**.

   The Role Catalog page opens.

3. In the **Display Name** field in the Search Roles section, enter the duty role’s display name and click **Search**.

4. In the Search Results section, select the duty role and select **New Policy - Default Policy Domain**.

   An Untitled tab opens.

5. In the Display Name field on the Untitled tab, enter the policy name. For example, enter Policy for Sales Department Management Duty.

---

**Tip**
Names of predefined security policies begin with the words Policy for.

6. In the Name field, enter the policy name. For example, enter SALES_DEPT_MANAGE_DUTY_POL.

7. In the Targets section, click **Add Targets**.
   The **Search Targets** dialog box opens.

**Tip**
In this context, a target is a function security privilege and a principal is a role. When a target is granted to the principal, a function security privilege is granted to the duty role.

8. In the **Display Name** field on the Entitlements tab, enter the name of the function security privilege. For example, enter Manage Department. Click **Search**.
   The Manage Department function security privilege secures access to the Manage Departments page.

9. In the search results, select the function security privilege and click **Add Selected**.
   This action adds the function security privilege to the Selected Targets section.

10. Click **Add Targets** to close the dialog box.
11. On the Untitled tab, click **Save**.
   This action updates the Untitled tab with the name of the new policy.

The next step is to assign data security policies to your custom duty role.

**Adding Data Security Policies to a Duty Role: Procedure**

This topic explains how to find the data security policies assigned to an existing duty role and add them to a custom duty role. Adding data security policies to a custom duty role is part of the process of creating the duty role. Typically, you perform this task immediately after adding function security privileges to a duty role.

**Adding Data Security Policies to a Duty Role**

If you are on the Authorization Management page, then click the Home tab and continue from step 3. Otherwise, sign 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.
The Oracle Entitlements Server Authorization Management page opens.

3. In the Application Name section of the Authorization Management Home tab, select hcm. Click Search under the Application Roles heading.

The Role Catalog page opens.

4. In the Display Name field in the Search Roles section, enter the name of the predefined duty role from which you want to copy the data security policies. For example, enter Department Management Duty. Click Search.

5. Select the role in the search results and click Open.

The Department Management Duty page opens.

6. In the top-right corner of the page, click Find Policies - Default Policy Domain.

The Search Authorization Policies tab opens.


The data security policies for this duty role appear on this tab.

8. Select the first data security policy of interest and click Edit.


The Select and Add: Roles dialog box opens.

Search for your duty role. For example, enter SALES_DEPT_MANAGE_DUTY in the Role Name field, select hcm as the Application, and click Search.

10. Select the duty role and click OK.

A copy of this data security policy now exists against your custom duty role.

11. Click Save. Click OK to close the Confirmation dialog box.

Repeat steps 8 through 11 to add additional data security policies to your duty role.

Verifying a Custom Duty Role : Procedure

Once you have created a custom duty role, you’re recommended to verify it. Typically, you perform this task immediately after adding function security privileges and data security policies to the duty role. This topic describes how to verify a custom duty role.

Verifying a Custom Duty Role

If you are on the Authorization Management page, then click the Home tab and continue from step 3. Otherwise, sign 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.

   The Oracle Entitlements Server Authorization Management page opens.

3. On the Home tab, select hcm in the Application Name section and click **Search** under the Application Roles header.

   The Role Catalog page opens.

4. Search for your duty role.

   In the search results, select the duty role and click **Open**. The duty role page opens.

5. Click **Find Policies - Default Policy Domain**.

   The Search Authorization Policies tab opens.

6. In the Policies For: section, the:

   a. Functional Policies tab shows your function security privileges.
   b. Data Security tab shows your data security policies.

7. Click **Close Multiple Tabs** to close the open tabs and return to the Home tab.

Next steps are to:

1. Add the new duty role to a job or abstract role.

2. Regenerate the data security policies for data or abstract roles that inherit this duty role.

---

### Regenerating HCM Data Roles: Procedure

You must regenerate a data or abstract role if you change its role hierarchy. For example, if you edit the duties of the job role that a data role inherits, then you must regenerate the data role. Regenerating a role updates its data security policies to reflect the latest role hierarchy. This procedure describes how to regenerate a role.

#### Regenerating a Role

To regenerate a data or abstract role:

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 Data Role and Security Profiles task.

3. On the Manage Data Roles and Security Profiles page, search for the data or abstract role.
4. Select the role in the Search Results and click **Edit**.

5. On the Edit Data Role: Select Role page, click **Next**.


7. On the Edit Data Role: Review page, click **Submit**.

This procedure automatically regenerates the role’s data security policies based on the security profiles assigned to the role.

To regenerate data security policies for multiple roles, you perform this task for each role.

---

**Note**

You must regenerate updated roles after each release upgrade of Oracle Fusion HCM.

---

### Enabling Access to HCM Audit Data: Points to Consider

This topic introduces ways of enabling access to HCM audit data.

#### Create a Data Role

You can create an HCM data role that includes the Internal Auditor job role with security profiles to identify the data that the role accesses. For example, to access audit data for person records, the HCM data role must include an appropriate person security profile. Use the predefined View All Workers security profile to enable access to audit data for all worker records.

#### Customize Job Roles

Your enterprise may allow other job roles, such as human resource specialist, to access audit data for the auditable business objects that they access. This approach requires customization of the job role itself to add the relevant duty roles. You include the job role in an HCM data role with one or more security profiles that identify the data.
Synchronizing User and Role Information with Oracle Identity Management

Synchronization of User and Role Information with Oracle Identity Management: How It's Processed

Oracle Identity Management (OIM) maintains Lightweight Directory Access Protocol (LDAP) user accounts for users of Oracle Fusion Applications. OIM also stores the definitions of abstract, job, and data roles, and holds information about roles provisioned to users.

Most changes to user and role information are shared automatically by Oracle Fusion Human Capital Management (Oracle Fusion HCM) and OIM. No action is necessary to make this exchange of information happen.

However, you must run the processes Send Pending LDAP Requests and Retrieve Latest LDAP Changes to manage some types of information exchange between Oracle Fusion HCM and OIM.

The table summarizes the role of each process.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to OIM. The response to each request from OIM to Oracle Fusion HCM indicates transaction status (for example, Completed).</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from OIM that may not have arrived automatically because of a failure or error, for example.</td>
</tr>
</tbody>
</table>

This figure summarizes the information flow of the daily processes.
Scheduling the Processes

You must run both processes at least daily to identify and process future-dated changes as soon as they take effect.

Retrieve Latest LDAP Changes must complete before Send Pending LDAP Requests runs. For this reason, leave a gap between the scheduled start times of the processes. Depending on the size of your enterprise and the number of updates, a gap of 1 or 2 hours may be enough.

Send Pending LDAP Requests has two required parameters, User Type and Batch Size. You’re recommended to use the default values of these parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Type</td>
<td>The types of users to be processed. Values are Person, Party, and All</td>
<td>All</td>
</tr>
<tr>
<td>Batch Size</td>
<td>The number of requests in a single batch. For example, if 400 requests exist and you set batch size to 25, then the process creates 16 batches of requests to process in parallel. The value A means that the batch size is calculated automatically.</td>
<td>A</td>
</tr>
</tbody>
</table>

Scheduling the LDAP Daily Processes: Procedure

You’re recommended to schedule these processes to run daily:

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to Oracle Identity Management (OIM).</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from OIM that may not have arrived automatically because of a failure or error, for example.</td>
</tr>
</tbody>
</table>
Important
Schedule the processes only when your implementation is complete. Once you schedule the processes, you can't run them on an as-needed basis, which is necessary during implementation.

This procedure explains how to schedule the processes.

Scheduling the Retrieve Latest LDAP Changes Process

1. Select Navigator - Tools - Scheduled Processes to open the Scheduled Processes work area.
2. Click Schedule New Process in the Search Results section of the Scheduled Processes work area.
4. In the Process Details dialog box, click Advanced.
5. On the Schedule tab, select Using a schedule.
6. In the Frequency field, select Daily.
7. Enter the start and end dates and times.
   Plan for Retrieve Latest LDAP Changes to complete before Send Pending LDAP Requests starts.
8. Click Submit.

Scheduling the Send Pending LDAP Requests Process

1. Click Schedule New Process in the Search Results section of the Scheduled Processes work area.
2. Search for and select the process Send Pending LDAP Requests in the Schedule New Process dialog box.
3. In the Process Details dialog box, select a user type value and enter a batch size. You're recommended to leave User Type set to All and Batch Size set to A.
   Click Advanced
4. On the Schedule tab, select Using a schedule.
5. In the Frequency field, select Daily.
6. Enter the start and end dates and times.
   Leave a gap between the start times of the two processes so that Retrieve Latest LDAP Changes completes before Send Pending LDAP Requests starts.
7. Click Submit.

Send Pending LDAP Requests: Explained

You're recommended to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to Oracle Identity Management (OIM). Schedule the process in the Scheduled Processes work area.
Send Pending LDAP Requests sends the following items to OIM:

- Requests to create, suspend, and reenable user accounts.
  - When you create a person record for a worker, a user-account request is generated automatically.
  - When a person has no roles and no current work relationships, a request to suspend the user account is generated automatically.
  - A request to reenable a suspended user account is generated automatically if you rehire a terminated worker.

The process sends these requests to OIM unless the automatic creation and management of user accounts are disabled for the enterprise.

- Work e-mails.
  If you include work e-mails when you create person records, then the process sends those e-mails to OIM, which owns them. They're usable only when OIM returns them to Oracle Fusion HCM.

- Role provisioning and deprovisioning requests.
  The process sends these requests to OIM unless automatic role provisioning is disabled for the enterprise.

- Changes to person attributes for individual users.
  The process sends this information to OIM unless the automatic management of user accounts is disabled for the enterprise.

- Information about HCM data roles, which originate in Oracle Fusion HCM.

**Note**

All of these items are sent to OIM automatically unless they’re either future-dated or generated by bulk data upload. You run the process Send Pending LDAP Requests to send future-dated and bulk requests to OIM.

---

**Retrieve Latest LDAP Changes: Explained**


You're recommended to run Retrieve Latest LDAP Changes daily. Schedule the process in the Scheduled Processes work area.

Retrieve Latest LDAP Changes delivers the following information to Oracle Fusion HCM from OIM:
• Names of user accounts.

   The globally unique identifier (GUID) from the LDAP directory user account is added automatically to the person record.

• Latest information about abstract, job, and data roles.

   OIM stores latest information about all abstract, job, and data roles, including HCM data roles. Oracle Fusion HCM keeps a local copy of all role names and types so that lists of roles in user interfaces are up to date.

---

**Note**

HCM data roles are available only after OIM returns them to Oracle Fusion HCM.

---

• Work e-mails.

   A worker can have only one work e-mail, which OIM owns. Once the e-mail exists, you manage it in OIM. Retrieve Latest LDAP Changes sends any changes to Oracle Fusion HCM.
Oracle Fusion Transactional Business Intelligence Security

Oracle Fusion Transactional Business Intelligence Security: Explained

Oracle Fusion Transactional Business Intelligence (OTBI) is a real-time, self-service reporting solution. All Oracle HCM Cloud service application users with appropriate roles can use OTBI to create analyses that support decision-making. Business users can perform current-state analysis of their business applications using a variety of tools. These include Oracle Business Intelligence Enterprise Edition (Oracle BI EE) as the standard query and reporting tool, Oracle Business Intelligence Answers (OBIA), and Oracle BI Dashboard end-user tools. This topic summarizes how access is secured to OTBI subject areas, Business Intelligence Catalog (BI Catalog) folders, and BI reports.

Subject Areas

Subject areas are functionally secured using duty roles. The names of duty roles that grant access to subject areas include the words Transaction Analysis Duty (for example, Workforce Transaction Analysis Duty). These duty roles exist under the obi application in Oracle Authorization Policy Manager (APM).

This table identifies the subject areas that predefined HCM job roles can access.

<table>
<thead>
<tr>
<th>HCM Job Role</th>
<th>Subject Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits Manager</td>
<td>All Benefits</td>
</tr>
<tr>
<td>Compensation Manager</td>
<td>All Compensation</td>
</tr>
<tr>
<td>Human Resource Analyst</td>
<td>Goals, Workforce Management, Workforce Performance, Workforce Profiles, and Talent Review</td>
</tr>
<tr>
<td>Line Manager</td>
<td>All Workforce Management</td>
</tr>
<tr>
<td>Payroll Manager</td>
<td>All Payroll</td>
</tr>
</tbody>
</table>
Analyses fail if the user can't access all subject areas in a report.

**Business Intelligence Catalog Folders**

BI Catalog folders are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Workforce Transaction Analysis Duty can access both the Workforce Management folder in the BI Catalog and the Workforce Management subject areas.

This table identifies the OTBI folders that predefined HCM job roles can access.

<table>
<thead>
<tr>
<th>HCM Job Role</th>
<th>OTBI Folders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits Manager</td>
<td>OTBI Benefits</td>
</tr>
<tr>
<td>Compensation Manager</td>
<td>OTBI Compensation</td>
</tr>
<tr>
<td>Human Resource Analyst</td>
<td>Business Intelligence Publisher (BIP) Goals, BIP Performance, BIP Profiles, OTBI Career, and OTBI Workforce Management folders</td>
</tr>
<tr>
<td>Line Manager</td>
<td>BIP Compensation, BIP Workforce Management, OTBI Workforce Management, and many OBIA folders</td>
</tr>
<tr>
<td>Payroll Manager</td>
<td>OTBI and OBIA Payroll folders</td>
</tr>
</tbody>
</table>

**BI Reports**

Analyses are secured based on the folders in which they’re stored. If you haven’t secured BI reports using the report privileges, then they’re secured at the folder level by default. You can set permissions against folders and reports in Oracle BI for Application Roles, Catalog Groups, or Users.

You can set permissions to:

- Read, Execute, Write, or Delete
- Change Permissions
- Set Ownership
- Run Publisher Report
- Schedule Publisher Report
- View Publisher Output

**Reporting Data Duty Roles: Explained**

The data that’s returned in Oracle Fusion Transactional Business Intelligence (OTBI) reports is secured in a similar way to the data that’s returned in Oracle Fusion HCM pages. Data access is granted by roles that are linked to security
profiles. This topic describes the part played by Reporting Data Duty Roles in securing access to data in OTBI reports. It also describes how to enable this access in custom job roles.

**Reporting Data Duty Roles**

Each of the Transaction Analysis Duty roles that grants access to subject areas and Business Intelligence Catalog (BI Catalog) folders inherits one or more Reporting Data Duty roles. These duty roles grant access to the data. The Reporting Data Duty roles are under the `hcm` application in Authorization Policy Manager (APM).

**Custom Job Roles**

If you create a custom job role with access to OTBI reports, then you must give the role both the `obi` and `hcm` versions of the Transaction Analysis Duty roles. These duty roles ensure that your custom job role has the function and data security for running the reports.

For example, if your custom role needs access to the Workforce Transaction Analysis subject areas, then it must inherit the following duty roles:

<table>
<thead>
<tr>
<th>Duty Role</th>
<th>APM Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce Transaction Analysis Duty</td>
<td>Under the <code>obi</code> application</td>
</tr>
<tr>
<td>Workforce Transaction Analysis Duty(HCM)</td>
<td>Under the <code>hcm</code> application</td>
</tr>
</tbody>
</table>

The Workforce Transaction Analysis Duty inherits the:

- Workforce Reporting Data Duty, providing access to person and assignment data
- Workforce Structures Reporting Data Duty, providing access to workforce structures
- Absence Management Reporting Data Duty, providing access to absence data
- Business Intelligence Authoring Duty, providing access to various features in Oracle Business Intelligence Answers (OBIA)

**Business Intelligence Roles: Explained**

Business Intelligence (BI) roles apply to both Business Intelligence Publisher (BI Publisher) and Oracle Fusion Transaction Business Intelligence (OTBI). They grant access to BI functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, BI catalog folders, and Oracle Fusion Human Capital Management data. This topic describes the BI roles.

BI roles are defined as application roles in Authorization Policy Manager (APM). This table identifies the BI roles.
<table>
<thead>
<tr>
<th>Business Intelligence Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI Consumer Role</td>
<td>Runs BI reports.</td>
</tr>
<tr>
<td>BI Author Role</td>
<td>Creates and edits reports.</td>
</tr>
<tr>
<td>BI Administrator Role</td>
<td>Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.</td>
</tr>
<tr>
<td>BI Publisher Data Model Developer Role</td>
<td>Creates and edits BI Publisher data models.</td>
</tr>
</tbody>
</table>

**BI Consumer Role**

You can configure custom roles to inherit BI Consumer Role so that they can run reports but not author them.

**BI Author Role**

The predefined OTBI Transaction Analysis Duty roles inherit BI Author Role. Therefore, users with these duty roles can create, edit, and run OTBI reports.

**BI Administrator Role**

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role. Therefore, users who can author reports can also run them. You’re recommended to provision this role to users in a test environment only.

None of the predefined HCM job roles has BI Administrator Role access.

**BI Publisher Data Model Developer Role**

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Therefore, users with either of these predefined job roles can manage BI Publisher data models.

**Viewing Reporting Roles and Permissions: Procedure**

Viewing reporting roles and permissions can help you to understand how Oracle Fusion Transactional Business Intelligence (OTBI) security works.

This topic explains how to view the:

- Transaction Analysis Duty roles that a job role inherits
- Permissions for sample OTBI reports in the Business Intelligence (BI) Catalog

**Viewing Transaction Analysis Duty Roles**

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.
   On the Home tab:
   a. In the Application Name section, select **hcm**.
   b. In the Search and Create section, click **Search - External Roles**.
      The Search - External Roles page opens.

3. In the **Display Name** field, enter the name of the job role. For example, enter **Human Resource Analyst** and click **Search**.
4. In the search results, select **Human Resource Analyst** and click **Open Role**.
   The Human Resource Analyst page opens.
5. Select the Application Role Mapping tab.
6. Expand the **hcm** folder.
   Notice the Transaction Analysis Duty roles, such as Documents of Record Transaction Analysis Duty(HCM), that this role inherits.
7. Expand the Absence Management Transaction Analysis Duty(HCM) role.
   It inherits the Absence Management Reporting Data Duty role and the Workforce Structures Reporting Data Duty role.
8. Collapse the **hcm** folder and expand the **obi** folder.
   Notice the Transaction Analysis Duty roles that appear here also.
10. Expand BI Author Role. It inherits BI Consumer Role.

**Viewing Permissions for OTBI Reports in the BI Catalog**

To view these permissions, you must have a role that inherits BI Administrator Role. None of the predefined HCM job roles inherits BI Administrator Role.

1. Select **Navigator - Tools - Reports and Analytics** to open the Reports and Analytics work area.
2. In the Contents pane, click **Browse Catalog**. The Business Intelligence Catalog page opens.
3. In the Folders pane, expand **Shared Folders**.
   Expand the **Human Capital Management** folder and then the **Payroll** folder.
4. Click the **Transaction Analysis Samples** folder.
   A list of reports appears in the BI Catalog page.
5. Under Costing Reports, click More - Permissions.

The Permissions dialog box opens. Scroll down to see the complete list of permissions, which includes the role BI Administrator Role.

6. Return to the Oracle Fusion Applications window and sign out.

---

**Business Intelligence Publisher Security**

**Business Intelligence Publisher Secured List Views: Explained**

Business Intelligence Publisher (BI Publisher) is a set of tools for creating formatted reports based on data models. You can access BI Publisher from BI Composer or the BI Catalog by clicking New - Report. This topic describes how you can use secured list views to secure access to data in BI reports.

Some reporting tools combine the data model, layout, and translation in one report file. With that approach, business intelligence administrators must maintain multiple copies of the same report to support minor changes. By contrast, BI Publisher separates the data model, layout, and translation. Therefore, BI reports can be:

- Generated and consumed in many output formats, such as PDF and spreadsheet
- Scheduled for delivery to e-mail, printers, and so on
- Printed in multiple languages by adding translation files
- Scheduled for delivery to multiple recipients

**BI Publisher Data Security and Secured List Views**

When you access data using a BI Publisher data model that uses an SQL Query as the data source, you have two options.

You can:

1. Select data directly from a database table, in which case the data you return isn’t subject to data-security restrictions. Because you can create data models on unsecured data using BI Publisher, you’re recommended to minimize the number of users who can create data models.

2. Join to a secured list view in your select statements. The data returned is determined by the security profiles that are assigned to the roles of the user who’s running the report.

The following table shows, for each database table:

- The secured list view
- The data security privilege required to report on data in the table, if it’s accessed using the secured list view
The duty role that has the security privilege

<table>
<thead>
<tr>
<th>Table</th>
<th>Secured List View</th>
<th>Data Security Privilege</th>
<th>Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>PER_ALL_PEOPLE_F</td>
<td>PER_PERSON_SECURED_LIST_V</td>
<td>PER_REPORT_PERSON_DATA</td>
<td>Person Reporting Duty</td>
</tr>
<tr>
<td>PER_PERSONS</td>
<td>PER_PUB_PERS_SECURED_LIST_V</td>
<td>PER_REPORT_PERSON_DEFERRED_DATA</td>
<td>Public Person Reporting Duty</td>
</tr>
<tr>
<td>PER_ALL_ASSIGNMENTS_M</td>
<td>PER_ASSIGNMENT_SECURED_LIST_V</td>
<td>PER_REPORT_ASSIGNMENT_DATA</td>
<td>Assignment Reporting Duty</td>
</tr>
<tr>
<td>HR_ALL_ORGANIZATION_UNITS_F</td>
<td>PER_DEPARTMENT_SECURED_LIST_V</td>
<td>PER_REPORT_DEPARTMENT_DATA</td>
<td>Workforce Structures Reporting Data Duty</td>
</tr>
<tr>
<td>HR_ALL_ORGANIZATION_UNITS_F</td>
<td>PER_LEGAL_EMP_SECURED_LIST_V</td>
<td>PER_REPORT_LEGAL_EMPLOYER_DATA</td>
<td>Legal Employer Reporting Duty</td>
</tr>
<tr>
<td>HR_ALL_POSITIONS_F</td>
<td>PER_POSITION_SECURED_LIST_V</td>
<td>PER_REPORT_POSITION_DATA</td>
<td>Workforce Structures Reporting Data Duty</td>
</tr>
<tr>
<td>PER_JOBS_F</td>
<td>PER_JOB_SECURED_LIST_V</td>
<td>PER_REPORT_HR_JOB_DATA</td>
<td>Workforce Structures Reporting Data Duty</td>
</tr>
<tr>
<td>PER_LOCATIONS</td>
<td>PER_LOCATION_SECURED_LIST_V</td>
<td>PER_REPORT_LOCATION_DATA</td>
<td>Workforce Structures Reporting Data Duty Human Resources Location Reporting Duty</td>
</tr>
<tr>
<td>PER_GRADES_F</td>
<td>PER_GRADE_SECURED_LIST_V</td>
<td>PER_REPORT_ASSIGNMENT_GRADE_DATA</td>
<td>Workforce Structures Reporting Data Duty</td>
</tr>
<tr>
<td>PER.LEGISLATIVE_DATA_GROUPS</td>
<td>PER_LDG_SECURED_LIST_V</td>
<td>PER_REPORT_LEGISLATIVE_DATA_GROUP_DATA</td>
<td>Legislative Data Reporting Duty</td>
</tr>
<tr>
<td>PAY_ALL_PAYROLLS_F</td>
<td>PER_PAYROLL_SECURED_LIST_V</td>
<td>PER_REPORT_PAYROLL_DEFINITION_DATA</td>
<td>Payroll Reporting Data Duty</td>
</tr>
<tr>
<td>CMP_SALARY</td>
<td>CMP_SALARY_SECURED_LIST_V</td>
<td>CMP_REPORT_SALARY_DATA</td>
<td>Compensation Reporting Data Duty</td>
</tr>
</tbody>
</table>

Note

PER_JOBS_F, PER_LOCATIONS, and PER_GRADES_F aren’t currently secured. The secured list views and privileges for these tables aren’t currently used.
When creating custom BI Publisher reports, you can find details of the secured list views in Oracle Enterprise Repository (OER). In the Assets pane, set the Type value to View and the Logical Business Area value to Human Capital Management.

**Business Intelligence Publisher and PII Data: Explained**

Personally identifiable information (PII) tables are secured at the database level using virtual private database (VPD) policies. Only authorized users can report on data in PII tables. This restriction also applies to Business Intelligence Publisher (BI Publisher) reports. The data in PII tables is protected using data security privileges that are granted by means of duty roles in the usual way. This topic identifies the Oracle Fusion Human Capital Management (Oracle Fusion HCM) tables that contain PII data and the data security privileges that are used to report on them.

**Oracle Fusion HCM PII Tables**

This table lists the Oracle Fusion HCM PII tables and the privileges that are used to report on data in these tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Data Security Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>PER_ADDRESSES_F</td>
<td>PER_REPORT_PERSON_ADDRESS_DATA</td>
</tr>
<tr>
<td>PER_DRIVERS_LICENSES</td>
<td>PER_REPORT_DRIVER_LICENSE_DATA</td>
</tr>
<tr>
<td>PER_EMAIL_ADDRESSES</td>
<td>PER_REPORT_PERSON_EMAIL_DATA</td>
</tr>
<tr>
<td>PER_NATIONAL_IDENTIFIERS</td>
<td>PER_REPORT_PERSON_NATIONAL_IDENTIFIER_DATA</td>
</tr>
<tr>
<td>PER_PASSPORTS</td>
<td>PER_REPORT_PERSON_PASSPORT_DATA</td>
</tr>
<tr>
<td>PER_PHONES</td>
<td>PER_REPORT_PERSON_PHONE_DATA</td>
</tr>
<tr>
<td>PER_VISAS_PERMITS_F</td>
<td>PER_REPORT_PERSON_VISA_DATA</td>
</tr>
</tbody>
</table>

**Note**

Work e-mail and phone aren't protected.

All of these privileges are accessible using the Workforce Reporting Data Duty role.
abstract role
A description of a person’s function in the enterprise that is unrelated to the person’s job (position), such as employee, contingent worker, or line manager. A type of enterprise role.

action
The kind of access named in a security policy, such as view or edit.

assignment
A set of information, including job, position, pay, compensation, managers, working hours, and work location, that defines a worker’s or nonworker’s role in a legal employer.

beneficiary
A person or organization designated to receive benefits from a compensation plan on the death of the plan participant.

business unit
A unit of an enterprise that performs one or many business functions that can be rolled up in a management hierarchy.

condition
An XML filter or SQL predicate WHERE clause in a data security policy that specifies what portions of a database resource are secured.

contingent worker
A self-employed or agency-supplied worker. Contingent worker work relationships with legal employers are typically of a specified duration. Any person who has a contingent worker work relationship with a legal employer is a contingent worker.

dashboard
A collection of analyses and other content, presented on one or more tabs, to help users achieve specific business goals.

data dimension
A stripe of data accessed by a data role, such as the data controlled by a business unit.

data instance set
The set of HCM data, such as one or more persons, organizations, or payrolls, identified by an HCM security profile.
**data role**
A role for a defined set of data describing the job a user does within that defined set of data. A data role inherits job or abstract roles and grants entitlement to access data within a specific dimension of data based on data security policies. A type of enterprise role.

**data security**
The control of access to data. Data security controls what action a user can take against which data.

**data security policy**
A grant of entitlement to a role on an object or attribute group for a given condition.

**database resource**
An applications data object at the instance, instance set, or global level, which is secured by data security policies.

**dependent**
A person who has a personal relationship with a participant in a compensation plan whom the participant designates to receive coverage through the plan.

**division**
A business-oriented subdivision within an enterprise. Each division is organized to deliver products and services or address different markets.

**document type**
A categorization of person documents that provides a set of options to control what document information to retain, who can access the documents, whether the documents require approval, and whether the documents are subject to expiry. A document type exists for a combination of document category and subcategory.

**duty role**
A group of function and data privileges representing one duty of a job. Duty roles are specific to applications, stored in the policy store, and shared within an Oracle Fusion Applications instance.

**effective start date**
For a date-effective object, the start date of a physical record in the object’s history. A physical record is available to transactions between its effective start and end dates.

**emergency contact**
Any of a person’s contacts whom the enterprise can call in an emergency.
enterprise
An organization with one or more legal entities under common control.

enterprise role
Abstract, job, and data roles are shared across the enterprise. An enterprise role is an LDAP group. An enterprise role is propagated and synchronized across Oracle Fusion Middleware, where it is considered to be an external role or role not specifically defined within applications.

entitlement
Grants of access to functions and data. Oracle Fusion Middleware term for privilege.

external role
See

function security
The control of access to a page or a specific widget or functionality within a page. Function security controls what a user can do.

gallery
A searchable collection of portraits that combines the functions of the person directory with corporate social networking and self-service applications for both workers and managers.

generic organization hierarchy
An organization hierarchy that includes organizations of all classifications.

HCM data role
A job role, such as benefits administrator, associated with instances of HCM data, such as all employees in a department.

HCM securing object
An HCM object that secures access to data in related objects. For example, access to specified person records allows access to data secured by person records, such as goal plans and evaluations.

job
A generic role that is independent of any single department or location. For example, the jobs Manager and Consultant can occur in many departments.

job role
A role for a specific job consisting of duties, such as an accounts payable manager or application implementation consultant. A type of enterprise role.
LDAP

LDG
Abbreviation for legislative data group.

legal employer
A legal entity that employs people.

legal entity
An entity identified and given rights and responsibilities under commercial law through the registration with a country’s appropriate authority.

legislative data group
A means of partitioning payroll and related data. At least one legislative data group is required for each country where the enterprise operates. Each legislative data group is associated with one or more payroll statutory units.

managed person
A person for whom a user can maintain some information. For example, line managers can maintain information about their direct and indirect reports.

nonworker
A person, such as a volunteer or retiree, who is not engaged in the core businesses of the enterprise or legal employer but who may receive payments from a legal employer. Any person who has a nonworker work relationship with a legal employer is a nonworker.

offering
A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

party
A physical entity, such as a person, organization or group, that the deploying company has an interest in tracking.

payroll flow pattern
A series of tasks performed in a predefined order, which are grouped into activities that represent the phases of the payroll process. The flow pattern is used to generate a payroll flow.

payroll statutory unit
A legal entity registered to report payroll tax and social insurance. A legal employer can also be a payroll statutory unit, but a payroll statutory unit can represent multiple legal employers.
pending worker
A person who will be hired or start a contingent worker placement and for whom you create a person record that is effective before the hire or start date.

person number
A person ID that is unique in the enterprise, allocated automatically or manually, and valid throughout the enterprise for all of a person's work and person-to-person relationships.

person type
A subcategory of a system person type, which the enterprise can define. Person type is specified for a person at the employment-terms or assignment level.

portrait
A selection of information about a worker or nonworker, including contact details, social connections, and activities and interests, that can be viewed and edited. Both the amount and type of information and the available actions depend on the role of the portrait user.

position
A specific occurrence of one job, fixed within one department, also often one location. For example, the position Finance Manager is an instance of the job Manager in the Finance Department.

public person
A person for whom basic information, such as name and phone, is available to all workers in worker directories and elsewhere.

role
Controls access to application functions and data.

role deprovisioning
The automatic or manual removal of a role from a user.

role hierarchy
Structure of roles to reflect an organization's lines of authority and responsibility. In a role hierarchy, a parent role inherits all the entitlement of one or more child roles.

role mapping
A relationship between one or more roles and one or more assignment conditions. Users with at least one assignment that matches the conditions qualify for the associated roles.
role provisioning
The automatic or manual allocation of a role to a user.

security profile
A set of criteria that identifies HCM objects of a single type for the purposes of securing access to those objects. The relevant HCM objects are persons, organizations, positions, countries, LDGs, document types, payrolls, and payroll flows.

security reference implementation
Predefined function and data security in Oracle Fusion Applications, including role based access control, and policies that protect functions, data, and segregation of duties. The reference implementation supports identity management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

segregation of duties
An internal control to prevent a single individual from performing two or more phases of a business transaction or operation that could result in fraud.

SQL predicate
A type of predicate using SQL to constrain the data secured by a data security policy.

system person type
A fixed name that the application uses to identify a group of people.

tax reporting unit
A legal entity that groups workers for the purpose of tax and social insurance reporting.

URL
Abbreviation for uniform resource locator.

work area
A set of pages containing tasks, searches, analytics, or other content that a user needs to accomplish a business goal. Most of the menu items within the Navigator represent work areas.

work relationship
An association between a person and a legal employer, where the worker type determines whether the relationship is a nonworker, contingent worker, or employee work relationship.
**XML filter**

A type of condition using XML to constrain the data secured by a data security policy.