

Oracle

Human Capital Management Cloud Securing Oracle HCM Cloud

Release 12

This guide also applies to on-premises
implementations

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

The business names used in this documentation are fictitious, and are not intended to identify any real companies currently or previously in existence.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Oracle customers that have purchased support 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.

Contents

Preface **i**

1 An Introduction to HCM Security in the Cloud **1**

Securing Oracle HCM Cloud: Overview	1
Role-Based Security: Explained	2
Predefined HCM Roles: Explained	4
Role Types: Explained	5
Role Inheritance: Explained	6
Duty Role Components: Explained	7
Aggregate Privileges: Explained	9
Security Customization: Points to Consider	10
Reviewing Predefined Roles: Explained	10
Oracle Fusion Applications Security Console: Explained	11

2 Creating Implementation Users **13**

HCM Implementation Users: Explained	13
Creating HCM Implementation Users: Overview	14
Synchronizing User and Role Information: Procedure	15
Importing Users and Roles into Applications Security: Procedure	16
Creating the TechAdmin Implementation User: Procedure	16
Creating the HCMUser Implementation User: Procedure	17

3 Creating HCM Data Roles for Implementation Users **21**

Overview	21
Creating the HRAnalyst_ViewAll Data Role: Procedure	21
Creating the HCMApplicationAdministrator_ViewAll Data Role: Procedure	22
Creating the HRSpecialist_ViewAll Data Role: Procedure	23
Creating HCM Data Roles for Workforce Compensation Implementation Users: Procedure	24
Creating HCM Data Roles for Global Payroll Implementation Users: Procedure	26

4	Enabling Basic Data Access for Abstract Roles	29
	Assigning Security Profiles to Abstract Roles: Explained	29
	Assigning Security Profiles to Abstract Roles: Worked Example	30
5	Assigning Roles to Implementation Users	33
	Creating a Role Mapping for HCM Implementation Data Roles: Procedure	33
	Assigning Abstract and Data Roles to HCMUser: Procedure	33
	Verifying HCMUser Access: Procedure	35
	Resetting the Cloud Service Administrator Sign-In Details: Procedure	35
6	Setting Up Applications Security	37
	Defining Security Synchronization Processes and Preferences: Overview	37
	Defining the Default User-Name Format: Explained	38
	Setting Password Policy: Explained	39
	Setting Role Preferences: Explained	40
	Managing User-Name and Password Notifications: Explained	42
	Creating a Custom Notification Template: Procedure	43
	Scheduling the Import User and Role Application Security Data Process: Procedure	44
	Importing User Login History: Explained	45
	Send Pending LDAP Requests: Explained	45
	Scheduling the Send Pending LDAP Requests Process: Procedure	46
	Running Retrieve Latest LDAP Changes: Procedure	47
	Bridge for Active Directory: Explained	48
7	Preparing for Application Users	49
	Overview	49
	User and Role-Provisioning Setup: Critical Choices	49
	User Account Creation Option: Explained	50
	User Account Role Provisioning Option: Explained	51
	User Account Maintenance Option: Explained	52
	User Account Creation for Terminated Workers Option: Explained	52
	Setting the User and Role Provisioning Options: Procedure	53
	Provisioning Abstract Roles to Users Automatically: Procedure	53
	FAQs for Preparing for Application Users	55

8	Creating Application Users	57
	Points to Consider	57
	Using the New Person Tasks: Procedure	57
	Using the Create User Task: Procedure	58
	FAQs for Creating Application Users	60
9	Managing Application Users	61
	Managing User Accounts: Procedure	61
	Changing User Names: Explained	62
	Sending Personal Data to LDAP: Explained	63
	Processing a User Account Request: Explained	64
	Linking Existing User Accounts to Person Records: Explained	65
	Suspending User Accounts: Explained	65
	Managing Application Users on the Security Console: Explained	67
	Providing Read-Only Access: Procedure	67
	FAQs for Managing Application Users	68
10	Provisioning Roles to Application Users	73
	Role Mappings: Explained	73
	Creating a Role Mapping: Procedure	74
	Role Mappings: Examples	76
	Role Provisioning and Deprovisioning: Explained	77
	Autoprovisioning: Explained	79
	Editing Role Mappings: Points to Consider	80
	FAQs for Provisioning Roles to Application Users	81
11	Reporting on Application Users and Roles	83
	Running the User Details System Extract Report: Procedure	83
	User Details System Extract Report Parameters	83
	User Details System Extract Report	84
	Person User Information Reports	86
	LDAP Request Information Reports	87
	Inactive Users Report	88
	User Role Membership Report	90
	User and Role Access Audit Report	91
	User Password Changes Audit Report	93
	FAQs for Reporting on Application Users and Roles	95

12 HCM Data Roles and Security Profiles 97

HCM Data Roles: Explained	97
HCM Security Profiles: Explained	98
Predefined HCM Security Profiles: Explained	100
Creating an HCM Data Role: Worked Example	100
Creating HCM Data Roles and Security Profiles: Points to Consider	103
Role Delegation: Explained	104
Enabling Role Delegation: Explained	106
Assigning Security Profiles to Job and Abstract Roles: Procedure	107
Configuring HCM Data Roles and Security Profiles for Audit: Procedure	108
Enabling Access to HCM Audit Data: Points to Consider	108
HCM Data Roles Configuration Diagnostic Test	109
HCM Security Profile Configuration Diagnostic Test	109
HCM Securing Objects Metadata Diagnostic Test	110
FAQs for HCM Data Roles and Security Profiles	110

13 Person Security Profiles 113

Securing Person Records: Points to Consider	113
Securing Person Records by Area of Responsibility: Procedure	116
Securing Person Records by Manager Hierarchy: Points to Consider	117
Specifying the Manager Type: Explained	119
Hierarchy Content: Explained	120
Securing Person Records Using Custom Criteria: Examples	121
Tables and Views in Custom Criteria: Explained	121
FAQs for Person Security Profiles	123

14 Organization and Other Security Profiles 125

Creating Organization Security Profiles: Examples	125
Securing Organizations: Points to Consider	125
Creating Position Security Profiles: Examples	126
Creating Document Type Security Profiles: Examples	127
Legislative Data Group Security Profiles: Explained	128
Creating Payroll Security Profiles: Examples	128
Creating Flow Pattern Security Profiles: Examples	129
Flow Security and Flow Owners: Explained	129
FAQs for Organization and Other Security Profiles	131



15	Using the Security Console	133
	Graphical and Tabular Role Visualizations: Explained	133
	Simulating Navigator Menus: Procedure	134
	Reviewing Role Assignments: Procedure	135
	Reviewing Role Hierarchies: Explained	136
	Comparing Roles: Procedure	136
	Reviewing Role Information on the Analytics Tab: Explained	137
16	Customizing Security	139
	Copying HCM Roles: Points to Consider	139
	Security Console Role-Copy Options: Explained	140
	Copying Upgraded Abstract Roles: Explained	141
	Copying Job or Abstract Roles: Procedure	141
	Editing Custom Job or Abstract Roles: Procedure	142
	Creating Job or Abstract Roles from Scratch: Procedure	144
	Copying and Editing Duty Roles: Procedure	145
17	Regenerating Roles	149
	Regenerating Roles: Explained	149
	Enabling the Grants Regeneration Process: Procedure	149
	Regenerating Multiple Data and Abstract Roles: Procedure	150
18	Security and Reporting	153
	Oracle Fusion Transactional Business Intelligence Security: Explained	153
	How Reporting Data Is Secured: Explained	154
	Business Intelligence Roles: Explained	155
	Viewing Reporting Roles and Permissions: Procedure	156
	Business Intelligence Publisher Secured List Views: Explained	157
	Business Intelligence Publisher and PII Data: Explained	159
	Dimension Security: Explained	160
	FAQs for Security and Reporting	160

19	Certificate Management	163
	Managing Certificates: Explained	163
	Generating Certificates: Explained	163
	Generating a Signing Request: Procedure	164
	Importing and Exporting X.509 Certificates: Procedure	164
	Importing and Exporting PGP Certificates: Procedure	165
	Deleting Certificates: Procedure	165
20	Role Optimization	167
	Role Optimizer: Explained	167
	Role Optimization Report	169
21	Advanced Data Security	173
	Advanced Data Security: Explained	173


Preface

This preface introduces information sources that can help you use the application.

Oracle Applications Help

Use the help icon  to access Oracle Applications Help in the application. If you don't see any help icons on your page, click the Show Help icon  in the global header. Not all pages have help icons. You can also access Oracle Applications Help at <https://fusionhelp.oracle.com>.

Using Applications Help

 **Watch:** This video tutorial shows you how to find help and use help features.

Additional Resources

- **Community:** Use [Oracle Applications Customer Connect](#) to get information from experts at Oracle, the partner community, and other users.
- **Guides and Videos:** Go to the [Oracle Help Center](#) to find guides and videos.
- **Training:** Take courses on Oracle Cloud from [Oracle University](#).

Documentation Accessibility

For information about Oracle's commitment to accessibility, see the [Oracle Accessibility Program](#).

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.

1 An Introduction to HCM Security in the Cloud

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.

Chapter	Contents
An Introduction to HCM Security in the Cloud	A brief overview of the concepts of role-based security and an introduction to the Oracle Fusion Applications Security Console
Creating Implementation Users	The role of implementation users and instructions for creating them
Creating HCM Data Roles for Implementation Users	How to provide the data access that enables implementation users to complete the functional implementation
Enabling Basic Data Access for Abstract Roles	How to provide basic data access for all employees, contingent workers, and line managers
Assigning Roles to Implementation Users	How to assign data and abstract roles to implementation users
Setting Up Applications Security	Setting enterprise options on the Security Console and maintaining the Oracle Fusion Applications Security tables.
Preparing for Application Users	Enterprise-wide options and related decisions that affect application users
Creating Application Users	The ways in which you can create application users, with instructions for some methods
Managing Application Users	How to maintain user accounts throughout the workforce life cycle
Provisioning Roles to Application Users	The ways in which application users can acquire roles, with instructions for creating some standard role mappings
Reporting on Application Users and Roles	Reporting on user accounts, inactive users, roles provisioned to users, and password changes

Chapter	Contents
HCM Data Roles and Security Profiles	How to create and manage HCM data roles and use HCM security profiles to identify the data that users can access
Person Security Profiles	How to secure access to person records
Organization and Other Security Profiles	How to secure access to organizations, positions, document types, legislative data groups, payrolls, and payroll flows
Using the Security Console	How to use the Security Console to review role hierarchies and role analytics
Customizing Security	How to copy predefined roles to create custom roles and how to create custom roles from scratch
Regenerating Roles	How to regenerate the data security policies of data and abstract roles when the role hierarchy changes
Security and Reporting	How to enable users to run Oracle Transactional Business Intelligence and Oracle Business Intelligence Publisher reports
Certificate Management	How to generate, import, export, and delete PGP and X.509 certificates for data encryption and decryption
Role Optimization	How to use the optional Role Optimization Report to analyze the role hierarchy for redundancies and other inefficiencies
Advanced Data Security	<p>An introduction to these optional cloud services:</p> <ul style="list-style-type: none"> • Database Vault for Oracle Fusion Human Capital Management Security Cloud Service • Transparent Data Encryption for Oracle Fusion Human Capital Management Security Cloud Service

During implementation, you can perform security-related tasks:

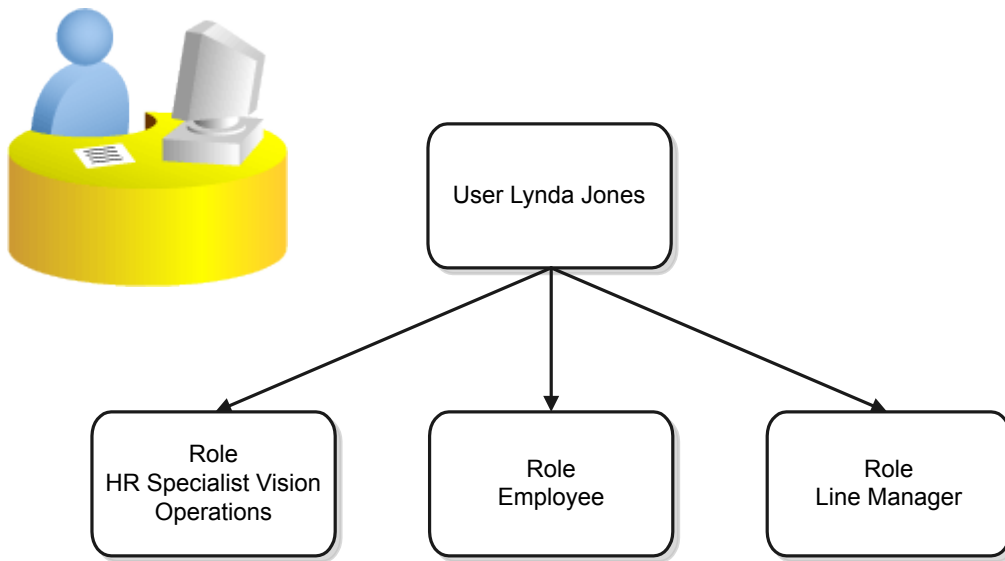
- From a functional area task list or an implementation project
- By selecting **Setup and Maintenance** from the Navigator and searching for the task in the Setup and Maintenance work area

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

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 Lynda Jones has three roles.



When Lynda signs in to Oracle Human Capital Management Cloud (Oracle HCM Cloud), she doesn't have to select a role. All of these roles are active concurrently.

The functions and data that Lynda can access are determined by this combination of roles.

- As an employee, Lynda can access employee functions and data.
- As a line manager, Lynda can access line-manager functions and data.
- As a human resource specialist (HR specialist), Lynda 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:

Component	Description
Who	Is a role assigned to a user
What	Is a function that users with the role can perform
Which Data	Is the set of data that users with the role can access when performing the function

For example:

Who	What	Which Data
Line managers	Can create performance documents	For workers in their reporting hierarchies
Employees	Can view payslips	For themselves
Payroll managers	Can report payroll balances	For specified payrolls
HR specialists	Can transfer workers	For workers in specified organizations

Predefined HCM Roles: Explained

Many job and abstract roles are predefined in Oracle Human Capital Management Cloud (Oracle HCM Cloud). 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 Capital Management Integration Specialist
- Human Resource Analyst
- Human Resource Manager
- Human Resource Specialist
- Line Manager
- Payroll Administrator
- Payroll Manager
- Power Recruiter
- Recruiting Administrator
- Time and Labor Administrator
- Time and Labor Manager

These predefined roles are part of the Oracle HCM Cloud 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 Human Capital Management Cloud (Oracle HCM Cloud) defines five types of roles:

- Data roles
- Abstract roles
- Job roles
- Aggregate privileges
- 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 Country Human Resource Specialist combines a job (human resource specialist) with a data scope (country). 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 HCM Cloud:

- Employee
- Contingent Worker
- Line Manager

You can also create custom abstract roles. All workers are likely to have at least one abstract role. Their abstract roles enable users to 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.

Aggregate Privileges

Aggregate privileges combine the functional privilege for an individual task or duty with the relevant data security policies. The functional privileges that aggregate privileges provide may grant access to task flows, application pages, work areas, reports,

batch programs, and so on. Job and abstract roles inherit aggregate privileges directly. Aggregate privileges don't inherit other roles. All aggregate privileges are predefined and you can't edit them. Although you can't create custom aggregate privileges, you can include the predefined aggregate privileges in custom job and abstract roles. You don't assign aggregate privileges directly to users.

Duty Roles

Each predefined duty role represents a logical grouping of privileges that you may want to copy and edit. Duty roles differ from aggregate privileges as follows:

- They include multiple function security privileges.
- They can inherit aggregate privileges and other duty roles.
- You can create custom duty roles.

Job and abstract roles may inherit duty roles either directly or indirectly. You can include predefined and custom duty roles in 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 many aggregate privileges. They may also inherit a few duty roles.

In addition to aggregate privileges and duty roles, job and abstract roles are granted many function security privileges and data security policies directly.

- Duty roles can inherit other duty roles and aggregate privileges.

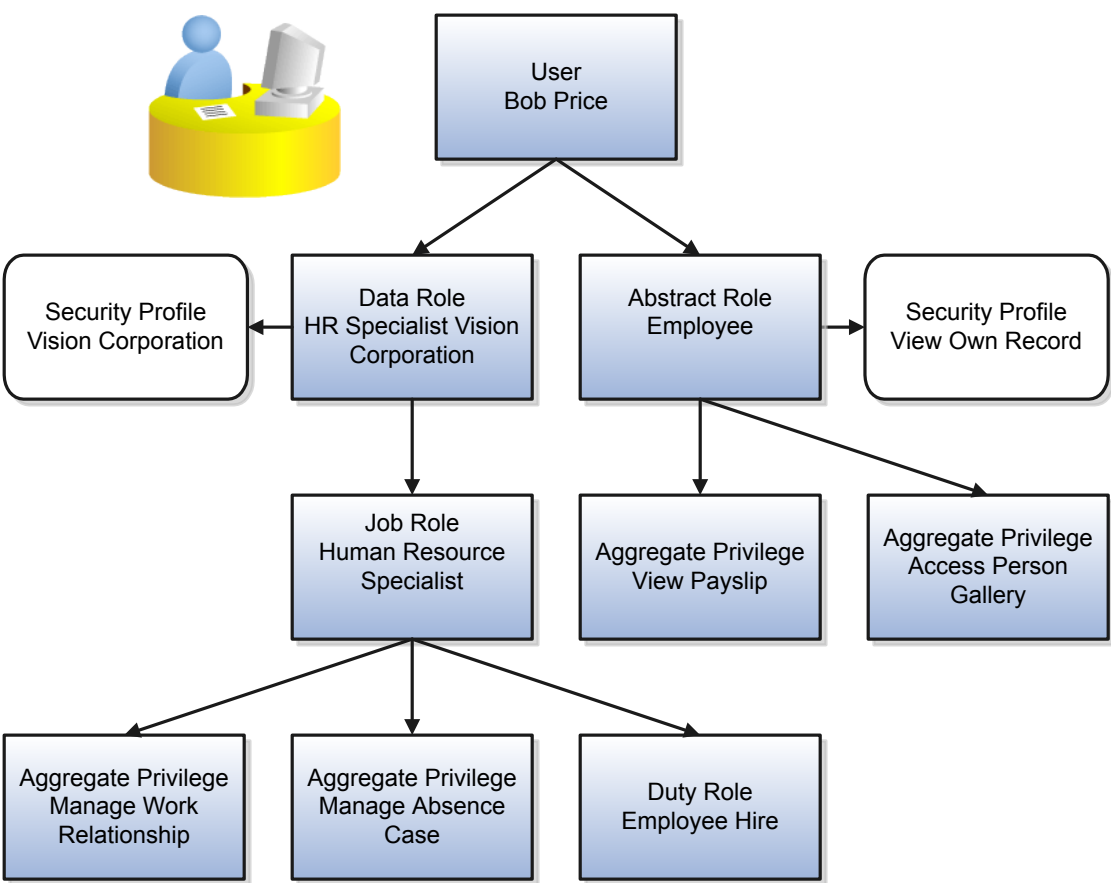
You can explore the complete structure of a job or abstract role on the Security Console.

When you assign data and abstract roles to users, they inherit all of 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 aggregate privileges and a single duty role. In reality, job and abstract roles inherit many aggregate privileges. Any duty roles that they inherit may themselves inherit duty roles and aggregate privileges.



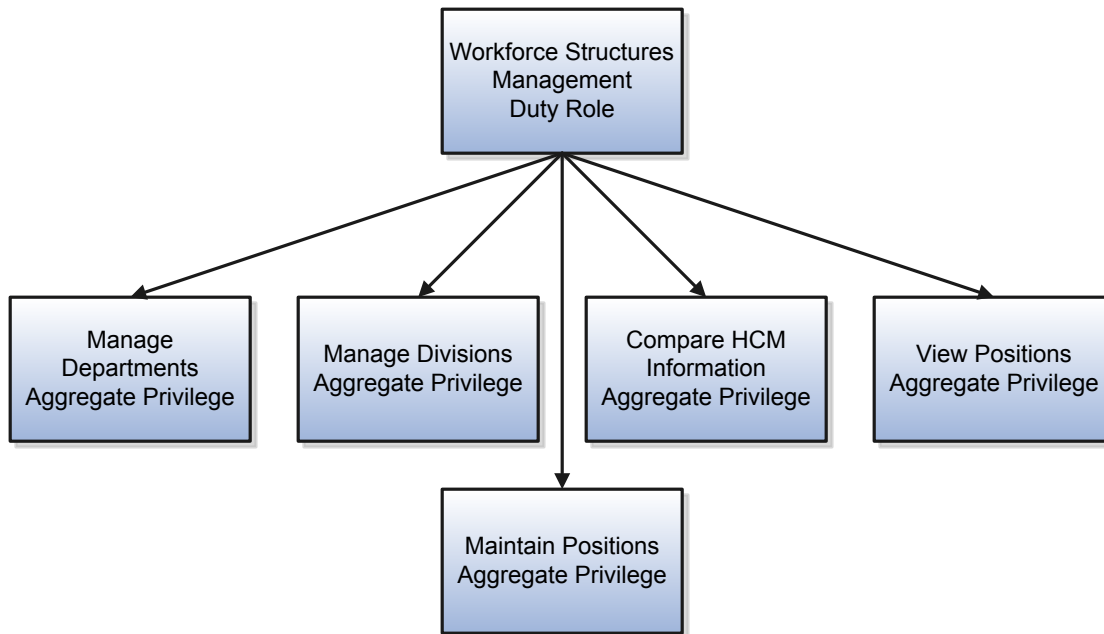
- In this example, user Bob Price has two roles:
- HR Specialist Vision Corporation, a data role
 - Employee, an abstract role

Role	Description
HR Specialist Vision Corporation	Inherits the job role Human Resource Specialist. This role inherits the aggregate privileges and 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 aggregate privileges and 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

This topic describes the components of a typical duty role. You must understand how duty roles are constructed if you plan to create custom duty roles, for example.

Function security privileges and data security policies are granted to duty roles. Duty roles may also inherit aggregate privileges and other duty roles. For example, the Workforce Structures Management duty role has the following structure.



In addition to its aggregate privileges, the Workforce Structures Management duty role is granted many function security privileges and data security policies.

Data Security Policies

Many data security policies are granted directly to the Workforce Structures Management duty role, including Manage Location, Manage Assignment Grade, and Manage HR Job. It also acquires data security policies indirectly, from its aggregate privileges.

Each data security policy combines:

- The role to which the data security policy is granted. The role can be a duty role, such as Workforce Structures Management, job role, abstract role, or aggregate privilege.
- A business object, such as assignment grade, that's being accessed. The data security policy identifies this resource by its table name, which is PER_GRADES_F for assignment grade.
- The condition, if any, that controls access to specific instances of the business object. Conditions are usually specified for resources that you secure using HCM security profiles. Otherwise, business object instances can be identified by key values. For example, a user with the Workforce Structures Management duty role can manage all grades in the enterprise.

- A data security privilege that defines permitted actions on the data. For example, Manage Assignment Grade is a data security privilege.

Function Security Privileges

Many function security privileges are granted directly to the Workforce Structures Management duty role, including Manage Location, Manage Assignment Grade, and Manage HR Job. It also acquires function security privileges indirectly, from its aggregate privileges.

Each function security privilege secures the code resources that make up the relevant pages, such as the Manage Grades and Manage Locations pages. Some user interfaces aren't subject to data security, so some function security privileges have no equivalent data security policy.

Predefined Duty Roles

The predefined duty roles represent logical groupings of privileges that you may want to manage as a group. They also represent real-world groups of tasks. For example, the predefined Human Resource Specialist job role inherits the Workforce Structures Management duty role. To create a custom Human Resource Specialist job role with no access to workforce structures, you would:

1. Copy the predefined job role.
2. Remove the Workforce Structures Management duty role from the copy.

Aggregate Privileges: Explained

Aggregate privileges are a type of role. Each aggregate privilege combines a single function security privilege with related data security policies. All aggregate privileges are predefined. This topic describes how aggregate privileges are named and used.

Aggregate Privilege Names

An aggregate privilege takes its name from the function security privilege that it includes. For example, the Promote Worker aggregate privilege includes the Promote Worker function security privilege.

Aggregate Privileges in the Role Hierarchy

Job roles and abstract roles inherit aggregate privileges directly. Duty roles may also inherit aggregate privileges. However, aggregate privileges can't inherit other roles of any type. As most function and data security below the level of job and abstract roles is provided by aggregate privileges, the role hierarchy has few levels. This flat hierarchy is easy to manage.

Use of Aggregate Privileges in Custom Roles

You can include aggregate privileges in the role hierarchy of a custom role. Treat aggregate privileges as role building blocks.

Customization of Aggregate Privileges

You can't create, edit, or copy aggregate privileges, nor can you grant the privileges from an aggregate privilege to another role. The purpose of an aggregate privilege is to grant a function security privilege only in combination with a specific data security policy. Therefore, you must use the aggregate privilege as a single entity.

If you copy a job or abstract role, then the source role's aggregate privileges are never copied. Instead, role membership is added automatically to the aggregate privilege for the copied role.

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 privileges. If some of your line managers don't handle compensation, then you can create a custom line manager role without those privileges. To create a custom role, you can either copy an existing role or create a role from scratch.

During implementation, you evaluate the predefined roles and decide whether changes are needed. You can identify predefined application roles easily by their role codes, which all have the prefix **ORA_**. For example, the role code of the Payroll Manager application job role is **ORA_PAY_PAYROLL_MANAGER_JOB**. All predefined roles are granted many function security privileges and data security policies. They also inherit aggregate privileges and duty roles. To make minor changes to a role, copying and editing the predefined role is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you create custom job roles. Add aggregate privileges and duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

If the privileges for a predefined job role don't match the corresponding job in your enterprise, then you create a custom version of the role. If you copy the predefined role, then you can edit the copy. You can add or remove aggregate privileges, duty roles, function security privileges, and data security policies, as appropriate.

Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you create custom duty roles. You can't create custom aggregate privileges. The typical implementation doesn't use custom duty roles.

Reviewing Predefined Roles: Explained

This topic describes some of the ways in which you can access information about predefined roles. This information can help you to identify which users need each role and whether to make any changes before provisioning roles.

The Security Console

On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.
- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

 **Tip:** The role codes of all predefined roles have the prefix **ORA_**.

Reports

You can run the User and Role Access Audit Report. This XML-format report identifies the function security privileges and data security policies for a specified role, all roles, a specified user, or all users.

The Security Reference Manuals

Two manuals describe the security reference implementation for Oracle HCM Cloud users:

- The Security Reference for Oracle Applications Cloud includes descriptions of all predefined security data that's common to Oracle Fusion Applications.
- The Security Reference for Oracle HCM Cloud includes descriptions of all predefined security data for Oracle HCM Cloud.

Both manuals contain a section for each predefined job and abstract role. For each role, you can review its:

- Duty roles and aggregate privileges
- Role hierarchy
- Function security privileges
- Data security policies

You can access the security reference manuals on docs.oracle.com.


Oracle Fusion Applications Security Console: Explained

The Oracle Fusion Applications Security Console is an easy-to-use administrative work area where you perform most security-management tasks. This topic introduces the Security Console and describes how to access it.

Security Console Functions

Use the Security Console to:

- Review role hierarchies and role analytics.

 **Note:** You can review HCM data roles on the Security Console. However, you must manage them on the Manage Data Roles and Security Profiles page.

- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.
- Create and manage implementation users and their roles.
- Compare roles.
- Simulate the Navigator for a user or role.

- Manage the default format of user names and the enterprise password policy.
- Manage notifications for user-lifecycle events, such as password expiration.
- Manage PGP and X.509 certificates for data encryption and decryption.
- Set up federation, and synchronize user and role information between Oracle Fusion Applications Security and Microsoft Active Directory, if appropriate.

Accessing the Security Console

You must have the IT Security Manager job role to access the Security Console. You open the Security Console by selecting **Tools - Security Console** from the home page or Navigator. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Manage Job Roles
- Manage Duties
- Create Implementation Users
- Revoke Data Role from Implementation Users

2 Creating Implementation Users

HCM Implementation Users: Explained

Implementation users:

- Manage the implementation of Oracle Human Capital Management Cloud (Oracle HCM Cloud).
- Administer application users and security, both during and after implementation.
- Set up basic enterprise structures.

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 HCM Cloud.

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:

Implementation User	Description
TechAdmin	Performs technical setup duties, including security setup. This user is intended for technical superusers.
HCMUser	Performs functional setup duties. This user is intended for users who are performing the Oracle HCM Cloud implementation steps.

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

- An application implementation 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.

 **Tip:** 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 HCM 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.

You're recommended to 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.

Accessing the Oracle HCM Cloud Service

The welcome or service-activation e-mail from Oracle provides the service URLs, user name, and temporary password for the test or production environment. Refer to the e-mail 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 welcome or service-activation e-mail. The URL ends with either **AtkHomePageWelcome** or **HcmFusionHome**.

When you sign in for the first time, use the password from the welcome or service-activation e-mail. You're prompted to change the password. 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.

Step	Task or Activity	Description
1	Run User and Roles Synchronization Process	You run the process Retrieve Latest LDAP Changes to copy data from your LDAP directory server to Oracle HCM Cloud.
2	Import Users and Roles into Application Security	You perform this task to initialize the Oracle Fusion Applications Security tables.
3	Create Implementation Users	You create the TechAdmin and HCMUser implementation users and assign required job roles to them if these users don't already exist in your environment.

Step	Task or Activity	Description
		You don't associate named workers with these users 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 two are required initially.
4	Create Data Roles for Implementation Users	<p>To enable implementation users to access HCM data, you create the following data roles:</p> <ul style="list-style-type: none"> • HRAnalyst_ViewAll • HCMApplicationAdministrator_ViewAll • HR_Specialist_ViewAll <p>You create additional data roles if you have licensed the Oracle Fusion Workforce Compensation Cloud Service or the Oracle Fusion Global Payroll Cloud Service.</p>
5	Assign Security Profiles to Abstract Roles	<p>Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles.</p> <p>You perform this task at this stage of the implementation so that implementation users with abstract roles have the required data access. However, all application users with abstract roles also benefit from this step.</p>
6	Create a Generic Role Mapping for HCM Data Roles	Enable the HCM data roles created in step 4 to be provisioned to implementation users.
7	Assign Abstract and Data Roles to the HCMUser Implementation User	Assign roles to the HCMUser implementation user that enable functional implementation to proceed.
8	Verify HCMUser Access	Confirm that the HCMUser implementation user can access the functions enabled by the assigned roles.

Reset your service administrator password after completing these steps.

Synchronizing User and Role Information: Procedure

You run the process Retrieve Latest LDAP Changes once during implementation. This process copies data from the LDAP directory to the Oracle Fusion Applications Security tables. Thereafter, the data is synchronized automatically. 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

Follow these steps:

1. Sign in to your Oracle Applications Cloud service environment as the service administrator.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Run User and Roles Synchronization Process task.
The process submission page for the Retrieve Latest LDAP Changes process opens.
4. Click **Submit**.
5. Click **OK** to close the confirmation message.

Importing Users and Roles into Applications Security: Procedure

To implement security, you must use the Security Console. Before you can use the Security Console, you must initialize the Oracle Fusion Applications Security tables with existing user and role information. To initialize these tables, you perform the Import Users and Roles into Application Security task. This topic describes how to perform this task.

Running the Import User and Role Application Security Data Process

Sign in as the Oracle HCM Cloud service administrator and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Import Users and Roles into Application Security task.
3. On the Import Users and Roles into Application Security page, click **Submit**.

This action starts the Import User and Role Application Security Data process. Once the process completes, you can use the Security Console.

 **Note:** You're recommended to schedule this process to run daily once your implementation users exist.

Related Topics

- [Scheduling the Import User and Role Application Security Data Process: Procedure](#)

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

Sign in as the Oracle HCM Cloud service administrator and follow these steps:


1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Create Implementation Users task.

The User Accounts page of the Security Console opens.

3. Click **Add User Account**.
4. Complete the fields on the Add User Account page as shown in the following table.

Field	Value
Associated Person Type	None
Last Name	TechAdmin
E-Mail	A valid e-mail for the user
User Name	TechAdmin
Password	Any value that complies with the password policy

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.


Assigning Roles to TechAdmin

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

1. In the Roles section of the Add User Account page, click **Add Role**.
2. In the **Add Role Membership** dialog box, search for the IT Security Manager job role.
3. In the search results, select the role and click **Add Role Membership**.
4. Click **OK** to close the **Confirmation** dialog box.
5. Repeat from step 2 to add each of the following job roles to the TechAdmin user:
 - Application Implementation Consultant
 - Application Diagnostics Administrator
 - Application Diagnostics Advanced User

Four job roles now appear in the Roles section of the Add User Account page.

6. Click **Save and Close**.

 **Note:** 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

Sign in as the Oracle HCM Cloud service administrator and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Create Implementation Users task.
The User Accounts page of the Security Console opens.
3. Click **Add User Account**.
4. Complete the fields on the Add User Account page as shown in the following table.

Field	Value
Associated Person Type	None
Last Name	HCMUser
E-Mail	A valid e-mail for the user
User Name	HCMUser
Password	Any value that complies with the password policy

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.


Assigning Roles to HCMUser

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

1. In the Roles section of the Add User Account page, click **Add Role**.
2. In the **Add Role Membership** dialog box, search for the Application Administrator job role.
3. In the search results, select the role and click **Add Role Membership**.
4. Click **OK** to close the **Confirmation** dialog box.
5. Repeat from step 2 to add each of the following job roles to the HCMUser user:
 - Application Implementation Consultant
 - Application Diagnostics Regular User
 - Application Diagnostics Viewer

Four job roles now appear in the Roles section of the Add User Account page.

6. Click **Save and Close**.

 **Note:** 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.

3 Creating HCM Data Roles for Implementation Users

Overview

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, 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 as the TechAdmin user. If this is the first use of this user name, then you're prompted to change the password. You use the new password whenever you sign in as this user subsequently.

Follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Assign Security Profiles to Role task.
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.

Field	Value
Data Role Name	HRAnalyst_ViewAll

Field	Value
Job Role	Human Resource Analyst

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Public Person	View All People
Document Type	View All Document Types
Payroll Flow	View All Flows

7. Click **Review**.
8. On the Create Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search for the HRAnalyst_ViewAll data role to confirm that it exists.

Creating the HCMApplicationAdministrator_ViewAll Data Role: Procedure

This topic describes how to create the HCMApplicationAdministrator_View All 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're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in as the TechAdmin user and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Assign Security Profiles to Role task.
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.

Field	Value
Data Role Name	HCMApplicationAdministrator_ViewAll
Job Role	Human Capital Management Application Administrator

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Public Person	View All People
Document Type	View All Document Types
Payroll	View All Payrolls
Payroll Flow	View All Flows

7. Click **Review**.
8. On the Create Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search for the HCMApplicationAdministrator_ViewAll data role to confirm that it exists.

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're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in as the TechAdmin user and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Assign Security Profiles to Role task.
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.

Field	Value
Data Role Name	HRSpecialist_ViewAll
Job Role	Human Resource Specialist

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Countries	View All Countries
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Public Person	View All People
Document Type	View All Document Types
Payroll	View All Payrolls
Payroll Flow	View All Flows

- Click **Review**.
- On the Create Data Role: Review page, click **Submit**.
- On the Manage Data Roles and Security Profiles page, search for the HRSpecialist_ViewAll data role to confirm that it exists.

Creating HCM Data Roles for 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 Assign Security Profiles to Role task.

Creating the CompensationAdmin_ViewAll Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in as the TechAdmin user and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Assign Security Profiles to Role task.
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.

Field	Value
Data Role Name	CompensationAdmin_ViewAll
Job Role	Compensation Administrator

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Payroll	View All Payrolls
Payroll Flow	View All Flows

7. Click **Review**.
8. On the Create Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search for the CompensationAdmin_ViewAll data role to confirm that it exists.

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.

Field	Value
Data Role Name	CompensationMgr_ViewAll

Field	Value
Job Role	Compensation Manager

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Countries	View All Countries
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Public Person	View All People
Document Type	View All Document Types
Payroll Flow	View All Flows

5. Click **Review**.
6. On the Create Data Role: Review page, click **Submit**.
7. On the Manage Data Roles and Security Profiles page, search for the CompensationMgr_ViewAll data role to confirm that it exists.

Creating HCM Data Roles for Global Payroll Implementation Users: Procedure

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

- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll

This topic explains how to create these roles using the Assign Security Profiles to Role task.

Creating the PayrollAdmin_ViewAll Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 3. Otherwise, sign in as the TechAdmin user and follow these steps:

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

2. Search for and select the Assign Security Profiles to Role task.
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.

Field	Value
Data Role Name	PayrollAdmin_ ViewAll
Job Role	Payroll Administrator

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Document Type	View All Document Types
Payroll	View All Payrolls
Payroll Flow	View All Flows

7. Click **Review**.
8. On the Create Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search for the PayrollAdmin_ ViewAll data role to confirm that it exists.

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.

Field	Value
Data Role Name	PayrollMgr_ ViewAll
Job Role	Payroll Manager

3. Click **Next**.

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

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People
Document Type	View All Document Types
Payroll	View All Payrolls
Payroll Flow	View All Flows

5. Click **Review**.
6. On the Create Data Role: Review page, click **Submit**.
7. On the Manage Data Roles and Security Profiles page, search for the PayrollMgr_ViewAll data role to confirm that it exists.

4 Enabling Basic Data Access for Abstract Roles

Assigning Security Profiles to Abstract Roles: Explained

These abstract roles are predefined in Oracle HCM Cloud:

- Employee
- Contingent Worker
- Line Manager


Users with these roles can sign in and open application pages. However, they have no automatic access to data. For example, employees can open the Directory but their searches return no results. Line managers can open the Directory 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 abstract roles.

Security Profile Type	Employee	Contingent Worker	Line Manager
Person	View Own Record	View Own Record	View Manager Hierarchy
Public person	View All Workers	View All Workers	View All Workers
Organization	View All Organizations	View All Organizations	View All Organizations
Position	View All Positions	View All Positions	View All Positions
Legislative data group	View All Legislative Data Groups	View All Legislative Data Groups	View All Legislative Data Groups
Country	View All Countries	View All Countries	View All Countries
Document type	View All Document Types	View All Document Types	View All Document Types
Payroll	Not applicable	Not applicable	View All Payrolls
Payroll flow	Not applicable	Not applicable	View All Flows

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.

 **Note:** 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 benefits representatives to access person records 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 Assign Security Profiles to Role task.

Searching for the Employee Abstract Role

1. Sign in as the TechAdmin user. On-premises users must sign in with a role that has the IT Security Manager job role.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Assign Security Profiles to Role task.
4. On the Manage Data Roles and Security Profiles page, enter Employee in the **Role** field. Click **Search**.
5. In the Search Results section, select the predefined Employee role and click **Edit**.

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 that you're implementing.

Field	Value
Organization Security Profile	View All Organizations
Position Security Profile	View All Positions
Country Security Profile	View All Countries
LDG Security Profile	View All Legislative Data Groups
Person Security Profile (Person section)	View Own Record

Field	Value
Person Security Profile (Public Person section)	View All Workers
Document Type Security Profile	View All Document Types

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 section, select the predefined Line Manager role and click **Edit**.

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 that you're implementing.

Field	Value
Organization Security Profile	View All Organizations
Position Security Profile	View All Positions
Country Security Profile	View All Countries
LDG Security Profile	View All Legislative Data Groups
Person Security Profile (Person section)	View Manager Hierarchy
Person Security Profile (Public Person section)	View All Workers
Document Type Security Profile	View All Document Types

Field	Value
Payroll	View All Payrolls
Payroll Flow	View All Flows

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.

5 Assigning Roles to Implementation Users

Creating a Role Mapping for HCM 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 - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage 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 **HR 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 **Autoprovision** options aren't selected.

 **Note:** If **Autoprovision** is selected automatically, then deselect it.

9. Repeat steps 7 and 8 for these 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**.

 **Note:** 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: 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.

Editing HCMUser

Follow these steps:

1. Sign in as the TechAdmin user.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Create Implementation Users task.
The User Accounts page of the Security Console opens.
4. On the User accounts page, search for the HCMUser implementation user.
5. In the search results, click the user name to open the User Account Details page.

These roles appear in the list of roles already assigned to HCMUser:

- o All Users
- o Application Administrator
- o Application Implementation Consultant
- o Application Diagnostics Regular User
- o Application Diagnostics Viewer

6. Click **Edit**.

Assigning Roles to HCMUser

Follow these steps:

1. In the Roles section of the User Account Details page, click **Add Role**.
2. In the **Add Role Membership** dialog box, search for the predefined Employee abstract role.
3. In the search results, select the role and click **Add Role Membership**.
4. Click **OK** to close the **Confirmation** dialog box.
5. Repeat from step 2 to add these abstract and HCM data roles to HCMUser:


- o Contingent Worker
- o Line Manager
- o HRSpecialist_ViewAll
- o HRAAnalyst_ViewAll
- o HCMApplicationAdministrator_ViewAll

If you have licensed the relevant cloud services and created these HCM data roles, then add them to HCMUser:

- o CompensationAdmin_ViewAll
- o CompensationMgr_ViewAll

- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll

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 **Delete**.

6. Click **Save and Close**.

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 using the HCMUser user name and password.
As this is the first use of this user name, you're prompted to change the password. HCMUser uses the new password to sign in subsequently.
2. Open the Navigator. In the Navigator, verify that:
 - Entries such as **Career Development**, **Goals**, and **Performance** appear under **My Workforce**, if you use Talent Management.
 - The **Compensation** entry appears, if you use Compensation Management.
 - The **Payroll** entries appear, if you use Global Payroll.
3. Sign out.

 **Tip:** You can also use the Security Console to verify user access. On the Roles tab, search for HCMUser. In the search results, select the user, right-click, and select **Simulate Navigator**. In the simulated navigator, any entry without a lock icon is available to the user.

HCMUser can now complete the functional implementation of Oracle HCM Cloud.

Resetting the Cloud Service Administrator Sign-In Details: Procedure

Once you have set up your implementation users, you can reset the service administrator sign-in details for your Oracle Applications Cloud service. You reset these details to avoid problems later when you're loaded to the 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 your Oracle Applications Cloud service using the TechAdmin user name and password and follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Create Implementation Users task.

The User Accounts page of the Security Console opens.

3. Search for your service administrator user name, which is typically your e-mail. Your service activation mail contains this value.
4. In the search results, click your service administrator user name to open the User Account Details page.
5. Click **Edit**.
6. Change the **User Name** value to **ServiceAdmin**.
7. Delete any value in the **First Name** field.
8. Change the value in the **Last Name** field to **ServiceAdmin**.
9. Delete the value in the **E-Mail** field.
10. Click **Save and Close**.
11. Sign out of your Oracle Applications Cloud service.

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

6 Setting Up Applications Security

Defining Security Synchronization Processes and Preferences: Overview

During implementation the TechAdmin user, who has the IT Security Manager job role, performs the tasks in the Define Security Synchronization Processes and Preferences task list. This topic introduces the tasks in this task list. They're described in more detail in this chapter.

Manage Application Security Preferences

This task opens the Administration tab of the Security Console.

On the General subtab of the Security Console Administration tab, you:

- Define the default format of user names for the enterprise.
- Set the enterprise password policy.
- Specify for how long certificates remain valid by default. Certificates establish keys for the encryption and decryption of data that Oracle HCM Cloud exchanges with other applications.
- Specify how often a warning appears to remind Security Console users to import latest user and role information.

On the Roles subtab of the Security Console Administration tab, you:

- Specify default prefix and suffix values for copied roles.
- Specify a limit to the number of nodes that can appear in graphical representations of roles on the Roles tab of the Security Console.
- Specify whether hierarchies on the Roles tab appear in graphical or tabular format by default.
- Manage editing of user-role memberships.
- Manage editing of data security policies.

On the Notifications subtab of the Security Console Administration tab, you:

- Manage the notification of user and password events to affected users.
- Define custom notification templates.

Import Users and Roles into Application Security

This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables. You're recommended to schedule this process to run daily.

Import User Login History

This task runs a process that imports the history of user access to Oracle Fusion Applications. This information is required by the Inactive Users Report.

Defining the Default User-Name Format: Explained

During implementation, you specify the default format of user names for the enterprise. This topic describes the available formats. To select a format, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. In the User Preferences section of this subtab, you select a user-name format. You can also change the enterprise format at any time on the Security Console. Select **Navigator - Tools - Security Console**.

User-Name Formats

This table describes the available user-name formats.

User-Name Format	Description
E-mail	<p>The work e-mail (or party e-mail, for party users) is the user name. For example, the user name for john.smith@example.com is john.smith@example.com. To make duplicate names unique, a number is added. For example, john.smith2@example.com may be used if john.smith@example.com and john.smith1@example.com already exist.</p> <p>E-mail is the default format.</p>
FirstName.LastName	<p>The user name is the worker's first and last names separated by a single period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user's middle name or a random character is used. For example, John Smith's user name could be john.frank.smith or john.x.smith.</p>
FLastName	<p>The user name is the worker's last name prefixed with the initial of the worker's first name. For example, the user name for John Smith is jsmith.</p>
Person or party number	<p>The party number or person number is the user name. If your enterprise uses manual person numbering, then any number that's entered during the hiring process becomes the user name. Otherwise, the number is generated automatically and can't be edited. The automatically generated number becomes the user name. For example, if John Smith's person number is 987654, then the user name is 987654.</p>


If you select a different user-name rule, then click **Save**. The change takes effect immediately.

System User Names

The selected user-name rule may fail. For example, a person's party number, person number, or e-mail may not be available when the user account is requested. In this case, a system user name is generated by applying these options in the following order until a unique user name is defined:

1. E-Mail
2. FirstName.LastName
3. If only the last name is available, then a random character is prefixed to the last name.

The Security Console option **Generate system user name when generation rule fails** controls whether a system user name is generated. You can disable this option. In this case, an error is raised if the user name can't be generated in the selected format.

 **Tip:** If a system user name is generated, then it can be edited later to specify a preferred value.

Editing User Names

Human resource (HR) specialists and line managers can enter user names in any format to override default user names when hiring workers. HR specialists can also edit user names for individual users on the Edit User and Manage User Account pages. The maximum length of the user name is 80 characters.

Work E-Mail

The line manager or HR specialist may omit the work e-mail when hiring the worker. In this case, the e-mail can't be added later by editing the worker details. However, you can edit the user on the Security Console and enter the e-mail there. To use work e-mail as the user name after a different user name has been generated, edit the existing user name.

Setting Password Policy: Explained


During implementation, you set the password policy for the enterprise. This topic describes the available options. To set the password policy, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. In the Password Policy section of this subtab, you select appropriate values. You can also change the enterprise policy at any time on the Security Console. Select **Navigator - Tools - Security Console**.

Password Policy Options

This table describes the available options for setting password policy.

Password-Policy Option	Description	Default Value
Days Before Password Expiration	Specifies the number of days for which a password remains valid. After this period, users must reset their passwords. By default, users whose passwords expire must follow the Forgot Password process.	90

Password-Policy Option	Description	Default Value
Days Before Password Expiry Warning	Specifies when a user is notified that a password is about to expire. By default, users are prompted to sign in and change their passwords. This value must be equal to or less than the value of the Days Before Password Expiration option.	80
Hours Before Password Reset Token Expiration	When users request a password reset, they're sent a password-reset link. This option specifies how long a reset-password link remains active. If the link expires before the password is reset, then reset must be requested again. You can enter any value between 1 and 9999.	4
Password Complexity	Specifies whether passwords must be simple, complex, or very complex. Password validation rules identify passwords that fail the selected complexity test.	Simple
Disallow last password	Select to ensure that the new password is different from the last password.	No
Administrator can manually reset password	Passwords can be either generated automatically or reset manually by the IT Security Manager or IT Auditor. Select this option to allow user passwords to be reset manually. All passwords, whether reset manually or generated automatically, must satisfy the current complexity rule.	Yes

 **Note:** Users are notified when passwords are about to expire, have already expired, or have been reset only if appropriate notification templates are enabled. The predefined notification templates for these events are Password Expiry Warning Template, Password Expiration Template, and Password Reset Template.

Password Expiry Report

The Password Expiry Report sends the password-expiration-warning and password-expired notifications. You must schedule the Password Expiry Report to run daily. To schedule the report:

1. Select **Navigators - Tools - Scheduled Processes**.
2. Click **Schedule New Process**.
3. In the **Schedule Process** dialog box, search for and select the Password Expiry Report process.
4. Click **OK**.
5. In the **Process Details** dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Select a **Frequency** value. For example, select **Daily**.
8. Select a start date and time.
9. Click **Submit**.

Setting Role Preferences: Explained

During implementation, you set default role preferences for the enterprise. This topic describes the role preferences and their effects. To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. From there, click the Roles subtab. You can also set role preferences at any time on the Security Console. Select **Navigator - Tools - Security Console**.

Copied-Role Names

To create custom roles, you're recommended to copy predefined roles and edit the copied roles. When you copy a predefined role:

- The **ORA_** prefix, which identifies predefined roles, is removed automatically from the role code of the copied role.
- The enterprise prefix and suffix values are added automatically to the role name and code of the copied role.

You specify enterprise prefix and suffix values on the Roles subtab of the Security Console Administration tab. By default:

- Prefix values are blank.
- The role-name suffix is **Custom**.
- The role-code suffix is **_CUSTOM**.

For example, if you copy the Benefits Administrator job role (ORA_BEN_BENEFITS_ADMINISTRATOR_JOB), then the default name and code of the copied role are:

- Benefits Administrator Custom
- BEN_BENEFITS_ADMINISTRATOR_JOB_CUSTOM

You can supply prefix values and change the suffix values, as required. If you change these values, then click **Save**. The changes take effect immediately.

Graph Nodes and Default Views

On the Roles tab of the Security Console, you can display role hierarchies. By default, these hierarchies appear in tabular format. To use graphical format by default, deselect the **Enable default table view** option on the Roles subtab of the Security Console Administration tab.

When role hierarchies appear on the Roles tab, the number of nodes can be very high. You can limit the number of nodes by setting the **Graph Node Limit** option on the Roles subtab of the Security Console Administration tab. When you display a role hierarchy with more nodes than the specified limit, gray arrows indicate additional nodes. You can set such a node as the focus node to see the rest of its hierarchy.

Data Security Policies and User Role Membership

By default, when creating or editing roles on the Security Console, you can manage their data security policies and assign the roles directly to users. These actions are controlled by the following options on the Roles subtab of the Security Console Administration tab:

- **Enable edit of data security policies**
- **Enable edit of user role membership**

Oracle HCM Cloud customers are recommended to disable these options. You're unlikely to have to edit data security policies directly, as they're generated automatically when you include security profiles in HCM data roles. If necessary, you can regenerate HCM data roles and abstract roles to which security profiles are assigned. For example, if you edit the security profiles in an HCM data role, then you regenerate the role to regenerate its data security policies.

To manage the automatic provisioning of roles to users, you create role mappings. Manual provisioning of roles to application users on the Security Console isn't recommended.

Related Topics

- [Copying HCM Roles: Points to Consider](#)
- [Role Provisioning and Deprovisioning: Explained](#)
- [Regenerating Roles: Explained](#)

Managing User-Name and Password Notifications: Explained

By default, users are notified automatically of changes to their user accounts and passwords. These notifications are based on notification templates. Many templates are predefined, and you can create custom templates. During implementation, you identify the notifications that you plan to use and disable any that aren't needed. This topic introduces the predefined notification templates and explains how to enable and disable notifications.

Predefined Notification Templates

This table describes the predefined notification templates. Each template is associated with a predefined event. For example, the Password Reset Template is associated with the password-reset event. You can see the notification templates and their associated events on the Notifications subtab of the Security Console Administration tab.

Notification Template	Description
Password Expiry Warning Template	Warns the user that a password is expiring soon and provides instructions for resetting the password.
Password Expiration Template	Notifies the user that a password has expired and provides instructions for resetting the password.
Forgot User Name Template	Sends the user name to a user who requested the reminder.
Password Generated Template	Notifies the user that a password has been generated automatically and provides instructions for resetting the password.
Password Reset Template	Sends a reset-password link to a user who performed the Reset Password action on the My Account page.
Password Reset Confirmation Template	Notifies the user when a password has been reset.
New Account Template	Notifies a user when a user account is created and provides a reset-password link.

Notification Template	Description
New Account Manager Template	Notifies the user's manager when a user account is created.

You're recommended not to edit the predefined templates, as your changes are lost on upgrade. However, you can create custom templates and disable the predefined versions. Each predefined event can be associated with only one enabled notification template at a time.

Enabling and Disabling Notifications

For any notification to be sent, notifications in general must be enabled. Ensure that the **Enable notifications** option on the Notifications subtab of the Security Console Administration tab is selected. When notifications are enabled, you can disable specific templates. For example, if you disable the New Account Template, then users aren't notified when their accounts are created. Other notifications continue to be sent.

To disable a template:

1. Select the template name on the Notifications subtab.
2. On the Edit Notification page, deselect the **Enabled** option.

Creating a Custom Notification Template: Procedure

Predefined notification templates exist for events related to the user-account life cycle, such as user-account creation and password reset. When templates are enabled, users are notified automatically of events that affect them. To provide custom notifications, you create custom notification templates. This topic explains how to create a custom notification template.

Creating a Notification Template

Follow these steps:

1. Select **Navigator - Tools - Security Console** to open the Security Console, and click the Administration tab.
2. Click the Notifications subtab on the Administration tab.
3. Click **Add Template**.
4. On the Add Notification Template page, enter the template name.
5. In the **Event** field, select a value. The predefined content for the selected event appears automatically in the **Message Subject** and **Message Text** fields. Tokens in the message text are replaced automatically in generated notifications with values specific to the user.
6. Update the **Message Subject** field, as required. The text that you enter here appears in the subject line of the notification e-mail.
7. Update the message text, as required. These tokens are supported in the message text.

Token	Meaning
notificationUserName	User name to which notifications are sent
userEmailAddress	Address to which e-mail notifications are sent
userLoginId	User name


Token	Meaning
firstName	User's first name
lastName	User's last name
managerFirstName	Manager's first name
managerLastName	Manager's last name
loginURL	URL where the user can sign in
resetURL	URL where the user can reset his or her password
CRLF	New line
SP4	Four spaces

8. To enable the template, select the **Enabled** option.
9. Click **Save and Close**.

 **Note:** When you enable a custom template for a predefined event, the predefined template for the same event is automatically disabled.

Scheduling the Import User and Role Application Security Data Process: Procedure

You must run the Import User and Role Application Security Data process to set up and maintain the Security Console. During implementation, you perform the Import Users and Roles into Application Security task to run this process. It copies users, roles, privileges, and data security policies from the LDAP directory, policy store, and Applications Core Grants schema to Oracle Fusion Applications Security tables. Having this information in the Oracle Fusion Applications Security tables makes the assisted search feature of the Security Console fast and reliable. After the process runs to completion for the first time, you're recommended to schedule Import User and Role Application Security Data to run daily. This topic describes how to schedule the process.

 **Note:** Whenever you run the process, it copies only those changes that were made since it last ran.

Scheduling the Process

Follow these steps to schedule the Import User and Role Application Security Data process:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.

3. In the **Schedule New Process** dialog box, search for and select the Import User and Role Application Security Data process.
4. Click **OK**.
5. In the **Process Details** dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times. The start time should be after any daily run of the Send Pending LDAP Requests process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.

Synchronization Process Preferences

On the General subtab of the Security Console Administration tab, you can set the **Synchronization Process Preferences** option. This option controls how frequently you're reminded to run the Import User and Role Application Security Data process. By default, the warning appears if the process hasn't run successfully in the last 6 hours. If you schedule the process to run daily, then you may want to increment this option to a value greater than 24.

Importing User Login History: Explained

During implementation, you perform the Import User Login History task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables. This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform Import User Login History for the first time, you're recommended to schedule it to run daily. In this way, you can ensure that the Inactive Users Report is up to date.

Scheduling the Import User Login History Process

Follow these steps:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the **Schedule New Process** dialog box, search for and select the Import User Login History process.
4. Click **OK**.
5. In the **Process Details** dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times.
9. Click **Submit**.
10. Click **OK** to close the **Confirmation** message.

Related Topics

- [Inactive Users Report](#)

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 your LDAP directory server. Schedule the process in the Scheduled Processes work area. This topic describes the purpose of Send Pending LDAP Requests.

Send Pending LDAP Requests sends the following items to the LDAP directory:

- Requests to create, suspend, and reactivate 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 reactivate a suspended user account is generated automatically if you rehire a terminated worker.

The process sends these requests to the LDAP directory 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 the LDAP directory.


- Role provisioning and deprovisioning requests.

The process sends these requests to the LDAP directory unless automatic role provisioning is disabled for the enterprise.

- Changes to person attributes for individual users.

The process sends this information to the LDAP directory unless the automatic management of user accounts is disabled for the enterprise.


- Information about HCM data roles, which originate in Oracle HCM Cloud.

 **Note:** All of these items are sent to the LDAP directory 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 the LDAP directory.

Only one instance of Send Pending LDAP Requests can run at a time.

Scheduling the Send Pending LDAP Requests Process: Procedure

The Send Pending LDAP Requests process sends bulk requests and future-dated requests that are now active to your LDAP directory. You're recommended to schedule the Send Pending LDAP Requests process to run daily. This procedure explains how to schedule the process.

 **Note:** Schedule the process only when your implementation is complete. Once you schedule the process you can't run it on an as-needed basis, which may be necessary during implementation.

Scheduling the Send Pending LDAP Requests Process

Follow these steps:

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.
3. In the **Schedule New Process** dialog box, search for and select the Send Pending LDAP Requests process.
4. In the **Process Details** dialog box, set **User Type** to identify the types of users to be processed. Values are **Person**, **Party**, and **All**. You're recommended to leave **User Type** set to **All**.
5. The **Batch Size** field specifies 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**, which means that the batch size is calculated automatically, is recommended.
6. Click **Advanced**.
7. On the Schedule tab, set **Run** to **Using a schedule**.
8. In the **Frequency** field, select **Daily**.
9. Enter the start and end dates and times.
10. Click **Submit**.

Running Retrieve Latest LDAP Changes: Procedure

Information about users and roles in your LDAP directory is available automatically to Oracle Cloud Applications. However, in specific circumstances you're recommended to run the Retrieve Latest LDAP Changes process. This topic describes when and how to run Retrieve Latest LDAP Changes.

You run Retrieve Latest LDAP Changes if you believe data-integrity or synchronization issues may have occurred between Oracle Cloud Applications and your LDAP directory server. For example, you may notice differences between roles on the Security Console and roles on the Create Role Mapping page. On-premises customers should also run this process after applying monthly updates.

Running Retrieve Latest LDAP Changes

Sign in 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 the **Refresh** icon.

Repeat this step periodically until the process completes.

 **Note:** Only one instance of Retrieve Latest LDAP Changes can run at a time.

Bridge for Active Directory: Explained

The bridge for Microsoft Active Directory synchronizes user account information between Oracle Applications Cloud and Microsoft Active Directory.

Using the Bridge for Microsoft Active Directory

To use the bridge for Active Directory and synchronize information between Oracle Applications Cloud and Active Directory, perform the following steps:

1. Configure the bridge for Active Directory. Set the configuration options on the Administration tab in the Security Console.
2. Map attributes between source and target applications for synchronization.
3. Download and install the bridge for Active Directory.
4. Perform initial synchronization of users.
5. Perform manual or automatic synchronization regularly to maintain consistency of data on the source and target applications.

Prerequisites

Before setting up the bridge between Active Directory and Oracle Applications Cloud, you must:

- Install Java Runtime environment (JRE). The bridge is compatible with JRE versions 6, 7, and 8.
- Install the bridge on a computer that can connect to your Active Directory server.
- Enable Single Sign-On (SSO) between Oracle Applications Cloud and your Active Directory instance.

Source and Target

The bridge synchronizes information between the source and target:

- Source: Is the application that contains the user and role information that is copied to the target.
- Target: Is the application that is updated to contain the same user and role information as the source.

You can select either Oracle Applications Cloud or Active Directory as the source.

Related Topics

- [Getting Started with Oracle Applications Cloud Bridge for Active Directory](#)

7 Preparing for Application Users

Overview

During implementation, you prepare your Oracle HCM 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 and introduced in this table.

Decision or Task	Topic
Whether user accounts are created automatically for application users	User Account Creation Option: Explained
How role provisioning is managed	User Account Role Provisioning Option: Explained
Whether user accounts are maintained automatically	User Account Maintenance Option: Explained
Whether user accounts are created for terminated workers that you load in bulk	User Account Creation for Terminated Workers Option: Explained
Ensuring that the Employee, Contingent Worker, and Line Manager abstract roles are provisioned automatically	Provisioning Abstract Roles to Users Automatically: Procedure

Some decisions affecting application users were made when the Security Console was set up. These decisions include:

- How user names are formed by default
- How passwords are formed and when they expire
- How users are notified of their sign-in details and password events, such as expiration warnings

You may want to review these settings on the Administration tab of the Security Console before creating application users.

Related Topics

- [Defining the Default User-Name Format: Explained](#)
- [Setting Password Policy: Explained](#)
- [Managing User-Name and Password Notifications: Explained](#)

User and Role-Provisioning Setup: Critical Choices

This topic introduces the user and role-provisioning options, which control the default management of some user-account features. To set these options, perform the Manage Enterprise HCM Information task in the Setup and Maintenance work area. 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 when you create a person, user, 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 Applications Cloud.
- Your existing provisioning infrastructure creates user accounts, and you plan to integrate it with Oracle Applications Cloud.

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.

 **Note:** Roles that you provision to users directly on the Security Console aren't affected by this option.

User Account Maintenance

The **User Account Maintenance** option controls whether user accounts are suspended and reactivated automatically. By default, a user's account is suspended automatically when the user is terminated and reactivated automatically if the user is rehired.

User Account Creation for Terminated Workers

The **User Account Creation for Terminated Workers** option controls whether user-account requests for terminated workers are processed or suppressed. This option takes effect when you run the Send Pending LDAP Requests process.

User Account Creation Option: Explained

The **User Account Creation** option controls whether user accounts are created automatically when you create a person or party record. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **User Account Creation** option values.

Value	Description
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 person records. Instead, account requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.
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 processed.

If user accounts are created automatically, then role provisioning also occurs automatically, as specified by current role mappings when the accounts are created. If user accounts aren't created automatically, then role requests are held in the LDAP requests table, where they're identified as suppressed. They aren't processed.

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

- Create user accounts individually on the Security Console.
- Link existing user accounts to person and party records using the Manage User Account or Manage Users task.

Alternatively, you can use an external provisioning infrastructure to create and manage user accounts. In this case, you're responsible for managing the interface with Oracle Applications Cloud, including any user-account-related updates.

User Account Role Provisioning Option: Explained

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, users may request some roles for themselves and acquire others automatically. All provisioning changes are role requests that are processed 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.

Value	Description
Both person and party users	Role provisioning and deprovisioning occur for both person and party users. This value is the default value.
Party users only	Role provisioning and deprovisioning occur for party users only. For person users, role requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.
None	For both person and party users, role requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.

User Account Maintenance Option: Explained

By default, a user's account is suspended automatically when the user has no roles. This situation occurs typically at termination. The user account is reactivated automatically if you reverse the termination or rehire the worker. 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.

Value	Description
Both person and party users	User accounts are maintained automatically for both person and party users. This value is the default value.
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. They're not processed. Select this value if you manage 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. They're not processed. Select this value if you manage accounts for both person and party users in some other way.

User Account Creation for Terminated Workers Option: Explained

The **User Account Creation for Terminated Workers** option controls whether user accounts are created for terminated workers. It applies only when you run Send Pending LDAP Requests. Typically, you run Send Pending LDAP Requests after loading workers in bulk using HCM Data Loader, for example. This option doesn't apply to workers created in the user interface unless they're future-dated. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **User Account Creation for Terminated Workers** option values.

Value	Description
No (or not set)	User-account requests generated for terminated workers are suppressed when you run Send Pending LDAP Requests.
Yes	User-account requests generated for terminated workers are processed when you run Send Pending LDAP Requests.

This option determines whether user-account requests for terminated workers are processed or suppressed. A user-account request is generated for a worker created by bulk upload only if:

- The **User Account Creation** enterprise option is set to **Both person and party users**.
- The **GeneratedUserAccountFlag** attribute for the Worker object isn't set to **N**.

Otherwise, user-account requests for workers are suppressed and **User Account Creation for Terminated Workers** has no effect.

Related Topics

- [Send Pending LDAP Requests: Explained](#)

Setting the User and Role Provisioning Options: Procedure

The user and role provisioning options control the creation and maintenance of user accounts for the enterprise. This procedure explains how to set these options. To create and maintain Oracle Applications Cloud user accounts automatically for all users, you can use the default settings.

Setting the User and Role Provisioning Options

Follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage Enterprise HCM Information task.
3. On the Enterprise page, select **Edit - Update**.
4. In the **Update Enterprise** dialog box, enter the effective date of any changes and click **OK**. The Edit Enterprise page opens.
5. Scroll down to the User and Role Provisioning Information section.
6. Set the User Account Options, as appropriate. The User Account Options are:
 - **User Account Creation**
 - **User Account Role Provisioning**
 - **User Account Maintenance**
 - **User Account Creation for Terminated Workers**

These options are independent of each other. For example, you can set **User Account Creation** to **None** and **User Account Role Provisioning** to **Yes**.

7. Click **Submit** to save your changes.
8. Click **OK** to close the **Confirmation** dialog box.

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. This topic explains how to set up automatic role provisioning during implementation using the Manage Role Provisioning Rules task.

Provisioning the Employee Role Automatically to Employees

Follow these steps:

1. Sign in as IT Security Manager or as the TechAdmin user.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Manage Role Provisioning Rules task. The Manage Role Mappings page opens.
4. In the Search Results section of the Manage Role Mappings page, click the **Create** icon. 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.

Field	Value
System Person Type	Employee
HR Assignment Status	Active

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, click **Search**.
9. In the **Search and Select** dialog box, enter Employee in the **Role Name** field and click **Search**.
10. Select Employee in the search results and click **OK**.
11. If **Autoprovision** isn't selected automatically, then select it. Ensure that the **Requestable** and **Self-Requestable** options aren't selected.
12. 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:

- In step 5, enter Contingent Worker as the mapping name.
- In step 6, set **System Person Type** to Contingent Worker.
- In steps 9 and 10, search for and select the Contingent Worker role.


Provisioning the Line Manager Role Automatically to Line Managers

Follow these steps:

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

Field	Value
System Person Type	Employee

Field	Value
HR Assignment Status	Active
Manager with Reports	Yes

 **Tip:** Setting **Manager with Reports** to Yes is the same as setting **Manager Type** to Line Manager. You don't need both values.

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, click **Search**.
6. In the **Search and Select** dialog box, enter Line Manager in the **Role Name** field and click **Search**.
7. Select Line Manager in the search results and click **OK**.
8. If **Autoprovision** isn't selected automatically, then select it. Ensure that the **Requestable** and **Self-Requestable** options aren't selected.
9. Click **Save and Close**.
10. On the Manage Role Mappings page, click **Done**.

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-on in the cloud?

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

Submit a service request for implementation of single sign-on. For more information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at <https://support.oracle.com>.

Related Topics

- [Oracle Applications Cloud Service Entitlements \(2004494.1\)](#)

8 Creating Application Users

Points to Consider

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

Some enterprises use applications 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. Oracle HCM Cloud user accounts 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 Data Loader

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 Workers Using HCM Data Loader

To load workers using HCM Data Loader, use the Import and Load Data task in the Data Exchange work area. The enterprise option **User Account Creation** controls whether user accounts are created for all workers by default. You can prevent user accounts from being created for individual workers by setting the **GeneratedUserAccountFlag** attribute of the user information component to **N**. You can also provide a user name in the uploaded data to override the default user-name format. You run the process Send Pending LDAP Requests to send bulk user-account requests for processing.

 **Note:** If appropriate role mappings don't exist when you load new workers, then user accounts are created but no roles are provisioned. User accounts without roles are automatically suspended when send Pending LDAP Requests completes. To avoid this suspension, always create a role mapping for the workers you're loading before you load them. Having the recommended role mapping to provision abstract roles automatically to employees, contingent workers, and line managers is sufficient in most cases.

Using the New Person Tasks: Procedure

Once your initial implementation of 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 Data 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: User-Name Values

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

1. Select **Navigator - My Workforce - New Person** to open the New Person work area.
2. On the Tasks panel tab, select the **Hire an Employee** task. 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 generation rule for user names, as specified on the Security Console, is **Person or party number**.

4. You enter the person's last name. Other names are optional. The user name is based on the person's first and last names if the generation rule for user names is either **FirstName.LastName** or **FLastName**.
5. Click **Next**. The Hire an Employee: Person Information page opens.
6. A user can have only one work e-mail. If you enter no work e-mail when you create the person record, then it can be entered later on the Security Console. You can't add it directly to the person record later. Once the person record exists, you manage the e-mail on the Security Console.

The user name is the work e-mail if the generation rule for user names is **E-Mail**.

7. Click **Next**.

Hiring an Employee: Roles

The Hire an Employee: Employment Information page opens. 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.

1. Click **Next**. The Hire an Employee: Compensation and Other Information page opens.
Any roles for which the employee qualifies automatically appear in the Role Requests region of the page.
2. To add roles manually, click **Add Role**. The **Add Role** dialog box opens.
3. Search for and select the role. A role that you can provision appears in a role mapping where you satisfy the conditions and the **Requestable** option is selected for the role.

The selected role appears in the Role Requests region with the status **Add requested**. Repeat steps 2 and 3 for additional roles.

4. Click **Next**. On the Hire an Employee: Review page, click **Submit**.

This action:

- Submits the Hire an Employee transaction for approval
- Creates a request to create the user account and provision the requested roles, on approval of the hire

The user is notified of his or her sign-in details if an appropriate notification template is enabled.

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.

. Sign in and follow these steps:

1. Select **Navigator - My Team - Manage Users** to open the Manage Users page.
2. In the Search Results section, click the **Create** icon.
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 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 is generated automatically and follows the enterprise default format.

Setting User Notification Preferences

The **Send user name and password** option controls whether a notification containing the new user's sign-in details is sent when the account is created. This option is enabled only if notifications are enabled on the Security Console and an appropriate notification template exists. For example, if the predefined notification template **New Account Template** is enabled, then a notification is sent to the new user.

If you deselect this option, then you can send the e-mail later by running the Send User Name and Password E-Mail Notifications process. An appropriate notification template must be enabled at that time.

Completing Employment Information

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

Adding Roles

1. Click **Autoprovision Roles**. Any roles for which the user qualifies automatically, based on the information that you have entered so far, 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. The role must appear in a role mapping for which you satisfy the role-mapping conditions and where the **Requestable** option is selected for the role.

The selected role appears in the Role Requests region with the status **Add requested**. The role request is created 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, an Oracle Fusion Applications user account is created automatically if automatic creation of accounts is enabled. If a user account isn't created automatically, then an authorized user can create it on the Security Console. You link an account created in this way to the person record on the Manage User Account page.

How can 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 the request is processed successfully, the account becomes available.

If automatic creation of accounts is disabled, then you can't use the Create User Account action. Instead, authorized users can create user accounts on the Security Console.

Where do default user names come from?

User names are generated automatically in the format specified on the Security Console. The default format is the worker's primary work e-mail, but this value can be overridden for the enterprise. For example, your enterprise may use person number as the default user name.

9 Managing Application Users

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. On the home page, select **My Workforce - Person Management** to open the Search Person page.
2. Search for the person whose account you're updating.
3. In the search results, select the person and select **Actions - Personal and Employment - 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 your LDAP directory server. Requests 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 - Autoprovision Roles**. This action applies to roles for which the **Autoprovision** 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 autoprovision roles for individual users if you know that additional or updated role mappings exist that affect those users.

Copying Personal Data to LDAP

By default, changes to personal data, such as person name and phone, are copied to your LDAP directory periodically. To copy any changes 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 notification containing a reset-password link to the user's work e-mail.


 **Note:** A notification template for the password reset event must exist and be enabled. Otherwise, no notification is sent.

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**. The maximum length of the user name is 80 characters.
3. Click **Save**.

This action sends the updated user name to your LDAP directory. Once the request is processed, 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 add roles, autoprovision roles, and copy their personal data to LDAP by selecting **About Me - My Account** from the home page. Line managers can add, remove, and autoprovision roles and copy personal data to LDAP for their reports from the Directory or by selecting **My Team** in the Navigator.

Changing User Names: Explained


By default, user names are generated automatically in the enterprise default format when you create a person record. Users who have the human resource specialist (HR specialist) role can change user names for existing HCM users whose records they can access. 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 available formats for Oracle HCM Cloud users.

User-Name Format	Description
E-Mail	The worker's work e-mail is the user name. If you don't enter the work e-mail when hiring the worker, then it can be entered later on the Security Console. This format is used by default. A different default format can be selected on the Administration tab of the Security Console.

User-Name Format	Description
FirstName. LastName	The user name is the worker's first and last names separated by a single period.
FLastName	The user name is the worker's last name prefixed with the initial of the worker's first name.
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.

 **Note:** If the default user-name rule fails, then a system user name can be generated. The option to generate a system user name is enabled by default but can be disabled on the Security Console.


Existing User Names

HR specialists can change an existing user name on the Manage User Account page.

To change a worker's user name:

1. Search for and select the worker in the Person Management work area.
2. For the selected worker, select **Actions - Personal and Employment - Manage User Account**.
3. On the Manage User Account page, select **Actions - Edit User Name**.

The updated name, which can be in any format, is sent automatically to your LDAP directory server. The maximum length of the user name is 80 characters.

 **Tip:** When you change an existing user name, the user's password and roles remain the same. However, 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

User accounts for users of Oracle Fusion Applications are maintained on your LDAP directory server. By default, Oracle HCM Cloud sends some personal information about users to the LDAP directory. This information includes the person number, person name, phone, and manager of the person's primary assignment. HCM Cloud shares these details to ensure that user-account information matches the information about users in HCM Cloud.

This topic describes how and when you can send personal information explicitly to your LDAP directory.

Bulk Creation of Users

After loading person records using HCM Data Loader, for example, you run the process Send Pending LDAP Requests. This process sends bulk requests for user accounts to the LDAP directory.

When you load person records in bulk, the order in which they're created in HCM Cloud 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 includes no manager details for the person in the user-account request. The LDAP directory information therefore differs from the

information that HCM Cloud holds for the person. To correct any differences between these versions of personal details, you run the Send Personal Data for Multiple Users to LDAP process.

The Send Personal Data for Multiple Users to LDAP Process

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

User Population	Description
All users	The process sends personal details for all users to the LDAP directory, regardless of whether they have changed since personal details were last sent.
Changed users only	The process sends only personal details that have changed since details were last sent to the LDAP directory (regardless of how they were sent). This option is the default setting.

 **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 Human Capital Management Application Administrator job role to run this process.

The Copy Personal Data to LDAP Action

Users can copy their own personal data to the LDAP directory from the Manage User Account page. Human resource specialists and line managers can also perform this action for users whose records they can access. By default, personal data changes are copied periodically to the LDAP directory. However, this action is available for copying changes immediately, if necessary.

Related Topics

- [User and Role-Provisioning Setup: Critical Choices](#)

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 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, then 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.

Linking Existing User Accounts to Person Records: Explained

By default, when you create person records, user accounts are created automatically in your LDAP directory and linked to those person records. However, this automatic creation of user accounts can be disabled for the enterprise. For example, you may have some other way of managing user accounts, or user accounts may already exist in your LDAP directory. In this case, you must link the user account manually to the person record. This topic explains how to link an existing user account to a person record in Oracle HCM Cloud. You must be able to access the person record to perform this task.

Linking an Existing User Account

Follow these steps:

1. On the home page, select **My Workforce - Person Management**.
2. Search for and select the worker.
3. For the selected worker, select **Actions - Personal and Employment - Manage User Account**.
4. On the Manage User Account page, select **Actions - Create User Account**.
This action is available only for workers who don't yet have a linked user account.
5. On the Manage User Account page, click **Link User Account**.
6. In the **Link User Account** dialog box, search for and select the user name.
The list contains only those user names that aren't already linked to an Oracle HCM Cloud person record.
7. Click **OK** to close the **Link User Account** dialog box.
8. Click **Save**.

This action links the user account to the person record. In addition, roles are provisioned to the user automatically as specified by current role-provisioning rules, unless automatic role provisioning is disabled for the enterprise. The Role Requests section of the Manage User Account page shows the roles for which the user qualifies. You can add roles, as appropriate, before clicking **Save**.

Suspending User Accounts: Explained

By default, user accounts are suspended automatically when a user has no roles. This automatic suspension of user accounts is controlled by the **User Account Maintenance** enterprise option. Human resource (HR) specialists can also

suspend a user account manually, if necessary. This topic describes how automatic account suspension and reactivation occur. It also explains how to suspend a user account manually.

Automatic Suspension of User Accounts

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 termination date or on the day following termination.

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.

Automatic Reactivation of User Accounts

User accounts are reactivated automatically when you reverse a termination or rehire a worker. If you reverse the termination of a work relationship, then:

- The user regains any role that he or she lost automatically at termination. For example, if the user automatically lost roles that had been provisioned manually, then those roles are reinstated.

 **Note:** 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 reactivated.

The autoprovisioning process runs automatically when you reverse a termination. Therefore, the user's roles are updated automatically as specified by current role mappings.

When you rehire a worker, the user account is reactivated automatically and roles are provisioned automatically as specified by current role mappings. In all other cases, you must reactivate suspended user accounts manually on the Edit User page.


 **Tip:** Authorized users can also manage user account status directly on the Security Console.

Manual Suspension of User Accounts

To suspend a user account manually, HR specialists follow these steps:

1. Select **Navigator - My Team - Manage Users**.
2. Search for and select the user to open the Edit User page.
3. In the User Details section of the Edit User page, set the **Active** value to **Inactive**. You can reactivate the account by setting the **Active** value back to **Active**.

4. Click **Save and Close**.

 **Note:** Role provisioning isn't affected by the manual suspension and reactivation of user accounts. For example, when you reactivate a user account manually, the user's autoprovisioned roles aren't updated unless you click **Autoprovision Roles** on the Edit User page. Similarly, a suspended user account isn't reactivated when you click **Autoprovision Roles**. You must explicitly reactivate the user account first.

IT security managers can lock user accounts on the Security Console. Locking a user account on the Security Console or setting it to **Inactive** on the Edit User page prevents the user from signing in.

Related Topics

- [User Account Maintenance Option: Explained](#)

Managing Application Users on the Security Console: Explained

Human resource specialists and line managers use the Manage User Account task for routine management of user accounts and role provisioning. Users can perform some tasks, such as requesting or delegating roles, on the My Account page. IT security managers can also manage user accounts, if appropriate. They perform relevant tasks on the User Accounts page of the Security Console. This topic summarizes the user-management tasks that IT security managers can perform.

User Management on the Security Console

On the User Accounts page of the Security Console, IT security managers can:

- Create and manage user accounts. Typically, only accounts for implementation users are created and managed in this way.
- Delete the account of an implementation user, if required. User accounts of application users should not be deleted.
- Lock and unlock user accounts. Users can't sign in to locked accounts.
- Make user accounts active or inactive.
- Reset user passwords, provided that the **Administrator can manually reset password** option on the Security Console Administration page is selected.

Providing Read-Only Access: Procedure

Some users may need read-only access to Oracle HCM Cloud. For example:

- A help desk representative must replicate a user's transaction without committing any changes.
- An auditor reviews application data for regulatory reasons but isn't authorized to change anything.

Read-only access is controlled by the Read Only Mode (FND_READ_ONLY_MODE) profile option. This topic describes how to set Read Only Mode for specific users.

Setting the Read Only Mode Profile Option

To enable read-only mode for a user:

1. Select **Navigator - Tools - Setup and Maintenance**.
2. In the Setup and Maintenance work area, search for and select the Manage Administrator Profile Values task.
3. In the Search section of the Manage Administrator Profile Values page, enter **FND_READ_ONLY_MODE** in the **Profile Option Code** field and click **Search**.
4. In the FND_READ_ONLY_MODE: Profile Values section of the page, click the **New** icon.
5. In the new row of the profile values table:
 - a. Set **Profile Level** to **User**.
 - b. In the **User Name** field, search for and select the user.
 - c. Set **Profile Value** to **Enabled** to activate read-only access for the selected user.
6. Click **Save and Close**.

When the user next signs in, a page banner reminds the user that read-only mode is in effect and no changes can be made.

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 did some roles appear automatically?

In a role mapping:

- The conditions specified for the role match the user's assignment attributes, such as job.
- The role has the **Autoprovision** option selected.

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, then 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, then 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 either for a specified period, such as a planned absence, or indefinitely.

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

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

The person keeps roles that were:

- Provisioned manually
- Acquired automatically for other active work relationships

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

Why does this worker have no user account?

Automatic creation of user accounts may be disabled in your enterprise. In this case, your enterprise may be managing user accounts outside Oracle HCM Cloud.

You can link an existing 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 your LDAP directory. Once the account status is **Active**, current roles appear in the Roles section of the Manage User Account or Edit User page. At this point, 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 your LDAP directory 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.

Only human resource specialists can edit user names.

What happens when I copy personal data to LDAP?

User accounts are defined in your LDAP directory. The LDAP directory also holds some personal information about users, such as name, work phone, and work location address. Changes to personal information in Oracle Human Capital Management Cloud are copied automatically at intervals to your LDAP directory. To send any changes 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 work e-mail of the user or user's line manager, if any. Notification templates for this event must exist and be enabled.

You can send these details once only for any user. If you deselect this option on the Manage User Account or Create User page, then 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 notification containing a reset-password link is sent to the user's work e-mail. A notification template for this event must exist and be enabled.

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

You can run the process Send User Name and Password E-Mail Notifications in the Scheduled Processes work area. For users for whom you haven't so far requested an e-mail, this process sends out user names and reset-password links. The e-mail goes to the 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. A notification template for this event must exist and be enabled.

Can I enable user impersonation?

No. The user impersonation feature (**Set Preferences - Proxies**) is disabled for Oracle Human Capital Management Cloud users. It can be enabled on request, but its use isn't recommended. User impersonation allows a proxy user uncontrolled access to the personal data of the impersonated user. The proxy user acquires all of that user's roles, which is unsafe if you use employee self-service.

10 Provisioning Roles to Application Users

Role Mappings: Explained

Roles give users 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. This topic describes how to provision roles to users both automatically and manually. Use the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area.

 **Note:** All role provisioning generates requests to provision roles. Only when those requests are processed successfully is role provisioning complete.

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.

Attribute	Value
Department	Finance Department
Job	Sales Manager
HR Assignment Status	Active

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

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.

Attribute	Value
Manager with Reports	Yes
HR Assignment Status	Active

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.

Attribute	Value
Department	Finance Department
System Person Type	Employee
HR Assignment Status	Active

Any user with at least one assignment that matches these conditions can request the role. 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 - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task.

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

Set values in the Conditions section to specify 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.

Field	Value
Department	Procurement Department
Job	Chief Buyer
Location	Denver
System Person Type	Employee
HR Assignment Status	Active

Users must have at least one assignment that meets all 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 HCM data role **Procurement Analyst Denver**.
3. Select one or more of the role-provisioning options:

Role-Provisioning Option	Description
Requestable	Qualifying users can provision the role to other users.
Self-Requestable	Qualifying users can request the role for themselves.

Role-Provisioning Option	Description
Autoprovision	Qualifying users acquire the role automatically.

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

 **Note:** **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**.

Applying Autoprovisioning

You're recommended to run the process Autoprovision Roles for All Users after creating or editing role mappings and after loading person records in bulk. This process compares all current user assignments with all current role mappings and creates appropriate autoprovioning requests.

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 request the Expenses Reporting data role.

You create a role mapping called All Employees and enter the following conditions.

Attribute	Value
System Person Type	Employee
HR Assignment Status	Active

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.

Attribute	Value
Business Unit	Sales
HR Assignment Status	Active
Manager with Reports	Yes

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.

 **Tip:** The **Manager with Reports** attribute always means a line manager. Setting the **Manager Type** attribute to **Line Manager** is the same as setting **Manager with Reports** to **Yes**. If your role mapping applies to managers of a type other than Line Manager, then don't set the **Manager with Reports** attribute.

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.

Attribute	Value
System Person Type	Retiree
HR Assignment Status	Inactive

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 Role Provisioning Rules or 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 data roles, abstract roles, and job roles to users. However, for Oracle HCM Cloud users, you typically include job roles in HCM data roles and provision those data roles.

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:

- On the termination date
- On the day after the termination date

If you enter a future termination date, then role deprovisioning doesn't occur until that date or the day after. The Role Requests in the Last 30 Days section on the Manage User Account page is updated only when the deprovisioning request is created. Entries remain in that section until they're processed.

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.

Reversal of Termination

Reversing a termination removes any roles that the user acquired automatically at termination. It also provisions roles to the user as follows:

- Any manually provisioned roles that were lost automatically at termination are reinstated.
- As the autoprovisioning process runs automatically when a termination is reversed, roles are provisioned automatically as specified by current role-provisioning rules.

You must reinstate manually any roles that you removed manually, if appropriate.

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.

Autoprovisioning: Explained

Autoprovisioning is the automatic allocation or removal of user roles. It occurs for individual users when you create or update assignments. You can also apply autoprovisioning explicitly for the enterprise using the Autoprovision Roles for All Users process. This topic explains the effects of applying autoprovisioning for the enterprise.

Roles That Autoprovisioning Affects

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.

The Autoprovision Roles for All Users Process

The Autoprovision Roles for All Users 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.

When a user has no roles, his or her user account is also suspended automatically by default.

The process creates requests immediately to add or remove roles. When running the process, you can specify when role requests are to be processed. You can either process them immediately or defer them as a batch to the next run of the Send Pending LDAP Requests process. Deferring the processing is better for performance, especially when thousands of role requests may be generated. Set the **Process Generated Role Requests** parameter to **No** to defer the processing. If you process the requests immediately, then Autoprovision Roles for All Users produces a report identifying the LDAP request ranges that were generated. Requests are processed on their effective dates.

When to Run the Process

You're recommended to run Autoprovision Roles for All Users after creating or editing role mappings. You may also have to run it after loading person records in bulk if you request user accounts for those records. If an appropriate role mapping exists before the load, then this process isn't necessary. Otherwise, you must run it to provision roles to new users loaded in bulk. Avoid running the process more than once in any day. Otherwise, the number of role requests that the process generates may slow the provisioning process.

Only one instance of Autoprovision Roles for All Users can run at a time.

Autoprovisioning for Individual Users

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

Related Topics

- [What happens when I autoprovision roles for a user?](#)
- [Scheduling the Send Pending LDAP Requests Process: Procedure](#)

Editing Role Mappings: Points to Consider

On the Edit Role Mapping page, you can update a role mapping. Changes that you make to start and end dates, role-mapping conditions, and the associated roles may affect current role provisioning. This topic describes when such changes take effect. To edit a role mapping, perform the Manage Role Provisioning Rules task in the Setup and Maintenance work area.

Making Changes to Roles That Were Provisioned Automatically

Changes to roles that were provisioned automatically take effect as soon as one of the following occurs:

- The Autoprovision Roles for All Users process runs.

This process compares all current user assignments with all current role mappings and updates role provisioning as appropriate. You're recommended to run this process after creating or editing role mappings and after loading person records in bulk.
- A human resource specialist (HR specialist) or line manager clicks **Apply Autoprovisioning** on the Manage User Account or Edit User page for individual users affected by the role mapping.

This action compares the user's current assignments with all current role mappings and updates the user's roles as appropriate.

- An HR specialist or line manager creates or updates assignments of users affected by the role mapping.

These actions cause a user's roles to be reevaluated.

Making Changes to Requestable Roles

Changes to requestable roles take effect immediately. If you remove a requestable role from the role mapping or change the role-mapping conditions, then:

- Users who currently have the role keep it.

Users such as line managers provision requestable roles manually to other users. 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.

- Users who could provision the role to other users can no longer do so, unless they satisfy any revised role-mapping conditions.

Making Changes to Self-Requestable Roles

Changes to self-requestable roles take effect immediately. If you remove a self-requestable role from the role mapping or change the role-mapping conditions, then:

- Users who currently have the role keep it.

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.

- Users who could request the role can no longer do so, unless they satisfy any revised role-mapping conditions.

FAQs for Provisioning Roles to Application Users

What's a role-mapping condition?

Most are assignment attributes, such as job or department. At least one of a user's assignments must match all assignment values in the role mapping for the user to qualify for the associated roles.

What's the difference between HR Assignment Status and Assignment Status?

Use **HR Assignment Status** to specify whether qualifying assignments must be active or inactive.

Use **Assignment Status** to specify a subcategory, such as **Active - Payroll Eligible** or **Suspended - No Payroll**.

When you select an **HR Assignment Status** value, the corresponding **Assignment Status** values appear. For example, if **HR Assignment Status** is **Inactive**, then **Assignment Status** values have the prefix Inactive or Suspended.

What's an associated role in a role mapping?

Any role that you want to provision to users. You can provision data roles, abstract roles, and job roles to users. The roles can be either predefined or custom.

What's the provisioning method?

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

Provisioning Method	Meaning
Automatic	The user qualifies for the role automatically based on his or her assignment attribute values.
Manual	Either another user assigned the role to the user, or the user requested the role.
External	The user acquired the role outside Oracle Applications Cloud.

11 Reporting on Application Users and Roles

Running the User Details System Extract Report: Procedure

The Oracle BI Publisher User Details System Extract Report includes details of selected Oracle Fusion Applications user accounts. To run this report, you must have a data role providing view-all access to person records for the Human Capital Management Application Administrator job role.

To run the report:

1. Select **Navigator - Tools - Reports and Analytics**.
2. In the Contents pane of the Reports and Analytics work area, select **Shared Folders - Human Capital Management - Workforce Management - Human Resources Dashboard**.
3. Select the User Details System Extract report.
4. In the report window, click **More**.
5. On the Oracle Business Intelligence page for the report, select either **Open** to run the report immediately or **More - Schedule** to schedule the report.

User Details System Extract Report Parameters

The Oracle BI Publisher User Details System Extract Report includes details of Oracle Fusion Applications user accounts. This topic describes the report parameters. Run the report in the Reports and Analytics work area. Select **Tools - Reports and Analytics** on the home page.

Parameters

User Population

Enter one of these values to identify user accounts to include in the report.

Value	Description
HCM	User accounts with an associated HCM person record.
TCA	User accounts with an associated party record.
LDAP	Accounts for users in the PER_USERS table who have no person number or party ID. Implementation users are in this category.
ALL	HCM, TCA, and LDAP user accounts.

From Date

Accounts for HCM and LDAP users that exist on or after this date appear in the report. If you specify no **From Date** value, then the report includes accounts with any creation date, subject only to any **To Date** value.

From and to dates don't apply to the TCA user population. The report includes all TCA users if you include them in the report's user population.

To Date

Accounts for HCM and LDAP users that exist on or before this date appear in the report. If you specify no **To Date** value, then the report includes accounts with any creation date, subject only to any **From Date** value.

From and to dates don't apply to the TCA user population. The report includes all TCA users if you include them in the report's user population.

User Active Status

Enter one of these values to identify the user-account status.

Value	Description
A	Include active accounts, which belong to users with current roles.
I	Include inactive accounts, which belong to users with no current roles.
All	Include both active and inactive user accounts.

User Details System Extract Report

The Oracle BI Publisher User Details System Extract Report includes details of Oracle Fusion Applications user accounts. This topic describes the report contents.

Run the report in the Reports and Analytics work area. Select **Tools - Reports and Analytics** on the home page.

Report Results

The report is an XML-formatted file where user accounts are grouped by type, as follows:

- Group 1 (G_1) includes HCM user accounts.
- Group 2 (G_2) includes TCA party user accounts.
- Group 3 (G_3) includes LDAP user accounts.

The information in the extract varies with the account type.

HCM User Accounts

Business Unit Name

The business unit from the primary work relationship.

Composite Last Update Date

The date when any one of a number of values, including assignment managers, location, job, and person type, was last updated.

Department

The department from the primary assignment.

Worker Type

The worker type from the user's primary work relationship.

Generation Qualifier

The user's name suffix (for example, Jr., Sr., or III).

Hire Date

The enterprise hire date.

Role Name

A list of roles currently provisioned to workers whose work relationships are all terminated. This value appears for active user accounts only.

Title

The job title from the user's primary assignment.

TCA User Accounts

Organizations

A resource group.

Roles

A list of job, abstract, and data roles provisioned to the user.

Managers

The manager of a resource group.

LDAP User Accounts

Start Date

The account's start date.

Created By

The user name of the user who created the account.

Person User Information Reports

This topic describes the Person User Dashboard and Person User Information Oracle Business Intelligence Publisher reports. Use these reports to extract information about the history of a specified Oracle HCM Cloud user account. To run the reports, you must have the IT Security Manager job role.

To run the reports:

1. Select **Navigator - Tools - Reports and Analytics** to open the Reports and Analytics work area.
2. In the Contents pane, select **Shared Folders - Human Capital Management - Workforce Management - Human Resources Dashboard**.

Both reports appear in the Human Resources Dashboard folder.

Running the Person User Information Reports

Use the Person User Dashboard report to display user account information, specifically the person ID, of a specified user. Follow these steps:

1. In the Human Resources Dashboard folder, click **Person User Dashboard - More**. The Oracle Business Intelligence Catalog page opens.
2. Find the Person User Dashboard entry on the Business Intelligence Catalog page and click **Open** to open the report.
3. On the Person User Dashboard page, complete the parameters in this table to filter the report and click **Apply**.

Parameter	Description
Display Name	Enter the user's display name, for example, John Gorman.
Last Name	Enter the user's last name, for example, Gorman.
Start Date	Enter the user's start date. Users with start dates equal to or later than this date may appear in the report.

4. Once you have identified the user of interest, copy the person ID from the Person User Information table in the report. You use this person ID in the Person User Information report.

Use the Person User Information report to display the detailed history of a specified user account. Follow these steps:

1. In the Human Resources Dashboard folder, click **Person User Information - More**. The Oracle Business Intelligence Catalog page opens.
2. Find the Person User Information entry on the Business Intelligence Catalog page and click **Open** to open the report.
3. On the Person User Information page, complete either or both of the parameters shown in this table and click **Apply**:

Parameter	Description
Start Date	Enter the user's start date. Users with start dates equal to or later than this date may appear in the report.
Person ID	Enter the person ID copied from the Person User Dashboard report.

The report output includes:

- Person information
- User history
- Assigned roles and details of the associated role mappings
- Role delegation details
- LDAP request details
- Work relationship and assignment information

To save either of the reports to a spreadsheet, select **Actions - Export - Excel**

LDAP Request Information Reports

This topic describes the LDAP Request Dashboard and LDAP Request Information reports. Use these reports to extract information about the status of LDAP requests. To run the reports, you must have the IT Security Manager job role.

To run the reports:

1. Select **Navigator - Tools - Reports and Analytics** to open the Reports and Analytics work area.
2. In the Contents pane, select **Shared Folders - Human Capital Management - Workforce Management - Human Resources Dashboard**.

Both reports appear in the Human Resources Dashboard folder.

Running the LDAP Request Information Reports

Use the LDAP Request Dashboard report to display summaries of requests in specified categories. Follow these steps:

1. In the Human Resources Dashboard folder, click **LDAP Request Dashboard - More**. The Oracle Business Intelligence Catalog page opens.
2. Find the LDAP Request Dashboard entry on the Business Intelligence Catalog page and click **Open** to open the report.
3. On the LDAP Request Dashboard page, complete the parameters in this table to filter the report and click **Apply**.

Parameter	Description
Within the Last N Days	Enter a number of days. The report includes LDAP requests updated within the specified period.
Request Type	Select an LDAP request type. The value can be one of Create, Update, Suspend, Activate, UserRoles, Terminate, and All.

Parameter	Description
Request Status	Select an LDAP request status. The value can be one of Complete, Faulted, In Progress, Request, Part Complete, Suppressed, Rejected, Consolidated, and All.

The report output includes:

- A summary of the enterprise settings for user-account creation and maintenance.
- Numbers of LDAP requests by status and type in both tabular and graphical formats.
- A summary table showing, for each request type, its status, equivalent user status, any error codes and descriptions, and the number of requests. All values are for the specified period.

You can refresh the report to update it as requests are processed.

Use the LDAP Request Information report to review details of the LDAP requests in the LDAP requests table in Oracle HCM Cloud. Follow these steps:

1. In the Human Resources Dashboard folder, click **LDAP Request Information - More**. The Oracle Business Intelligence Catalog page opens.
2. Find the LDAP Request Information entry on the Business Intelligence Catalog page and click **Open** to open the report.
3. On the LDAP Request Information page, complete the parameters in this table to filter the report and click **Apply**.

Parameter	Description
Within the Last N Days	Enter a number of days. The report includes LDAP requests updated within the specified period.
Request Type	Select an LDAP request type. The value can be one of Create, Update, Suspend, Activate, UserRoles, Terminate, and All.
Request Status	Select an LDAP request status. The value can be one of Complete, Faulted, In Progress, Request, Part Complete, Suppressed, Rejected, Consolidated, and All.

The report includes a table showing for each request:

- The request date and type
- Whether the request is active
- The request status and its equivalent user status
- Error codes and descriptions, if appropriate
- Requested user names, if any
- The person to whom the request relates
- When the request was created and last updated


To save either of the reports to a spreadsheet, select **Actions - Export - Excel**.

Inactive Users Report

Run the Inactive Users Report to identify users who haven't signed in for a specified period.

To run the report:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the Import User Login History process.

 **Note:** Whenever you run the Inactive Users Report process, you must first run the Import User Login History process. This process imports information that the Inactive Users Report process uses to identify inactive users. You're recommended to schedule Import User Login History to run daily.

4. When the Import User Login History process completes, search for and select the Inactive Users Report process.
5. In the **Process Details** dialog box, set parameters to identify one or more users.
6. Click **Submit**.

Inactive Users Report Parameters

All parameters except **Days Since Last Activity** are optional.

User Name Begins With

Enter one or more characters.

First Name Begins With

Enter one or more characters.

Last Name Begins With

Enter one or more characters.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Days Since Last Activity

Enter the number of days since the user last signed in. Use this parameter to specify the meaning of the term inactive user in your enterprise. Use other parameters to filter the results.

This value is required and is 30 by default. This value identifies users who haven't signed in during the last 30 or more days.

Last Activity Start Date

Specify the start date of a period in which the last activity must fall.

Last Activity End Date

Specify the end date of a period in which the last activity must fall.

Viewing the Report

The process produces an `Inactive_Users_List_processID.xml` file and a `Diagnostics_processID.zip` file.

The report includes the following details for each user who satisfies the report parameters:

- Number of days since the user was last active
- Date of last activity
- User name
- First and last names
- Assignment department
- Assignment location
- City and country
- Report time stamp

Related Topics

- [Importing User Login History: Explained](#)

User Role Membership Report


The User Role Membership Report lists role memberships for specified users.

To run the report process:

1. Select **Navigator - Tools - Scheduled Processes**.
2. In the Scheduled Processes work area, search for and select the User Role Membership Report process.

User Role Membership Report Parameters

You can specify any combination of the following parameters to identify the users whose role memberships are to appear in the report.

 **Note:** The report may take a while to complete if you run it for all users, depending on the number of users and their roles.

User Name Begins With

Enter one or more characters of the user name.

First Name Begins With

Enter one or more characters from the user's first name.

Last Name Begins With

Enter one or more characters from the user's last name.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Viewing the Report

The process produces a `UserRoleMemberships_processID_CSV.zip` file and a `Diagnostics_processID.zip` file. The `UserRoleMemberships_processID_CSV.zip` file contains the report output in CSV format. The report shows the parameters that you specified, followed by the user details for each user in the specified population. The user details include the user name, first and last names, user status, department, location, and role memberships.

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console. This report is based on data in the Applications Security tables, which you populate by running the Import User and Role Application Security Data process.

To run the User and Role Access Audit Report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the User and Role Access Audit Report.
3. In the **Process Details** dialog box, set parameters and click **Submit**.
4. Click **OK** to close the confirmation message.

User and Role Access Audit Report Parameters

Population Type

Set this parameter to one of these values to run the report for one user, one role, multiple users, or all roles.

- **All roles**
- **Multiple users**
- **Role name**
- **User name**

User Name

Search for and select the user name of a single user.

This field is enabled only when **Population Type** is **User name**.

Role Name

Search for and select the name of a single aggregate privilege or data, job, abstract, or duty role.

This field is enabled only when **Population Type** is **Role name**.

From User Name Starting With

Enter one or more characters from the start of the first user name in a range of user names.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of multiple users.

To User Name Starting With

Enter one or more characters from the start of the last user name in a range of user names.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of multiple users.


User Role Name Starts With

Enter one or more characters from the start of a role name.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of all users and roles.

Data Security Policies

Select the **Data Security Policies** check box, when you want to view the data security report for any population. When you leave the option unchecked, only the function report is generated.

 **Note:** If you don't need the data security policy document, leave the option unchecked. This reduces the processing time to run the report.

Debug

Select the **Debug** check box to include role GUID in the report. The role GUID is used to troubleshoot. Use this option only when requested by the Oracle Support team.

Viewing the Report Results


The report produces one or two **.zip** files depending on the parameters you select. When you select the Data Security Policies check box, two **.zip** files are generated: one with information on the data security policies and the other on functional security policies in a hierarchical format.

The file names are in the following format: [FILE_PREFIX]_[PROCESS_ID]_[DATE]_[TIME]_[FILE_SUFFIX]. The file prefix depends on the specified **Population Type** value, as shown in this table.

Population Type	File Prefix
User name	USER_NAME
Role name	ROLE_NAME
Multiple users	MULTIPLE_USERS
All roles	ALL_ROLES

This table shows the file suffix, file format, and file contents for each population type.

Population Type	File Suffix	File Format	File Contents
Any	DataSec	CVS	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when the Data Security Policies check box is selected.
Any	Hierarchical	CVS	Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.
Multiple users	CSV	CSV	Functional security policies in a comma-separated, tabular format.
All roles			

 **Note:** Extract the data security policies only when needed as it takes a long time to generate the file.

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547 and the Data Security Policies option selected, then the report files are:

- ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip
- ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip
- Diagnostic.zip

User Password Changes Audit Report

This report identifies users whose passwords were changed in a specified period. You must have the `ASE_USER_PASSWORD_CHANGES_AUDIT_REPORT_PRIV` function security privilege to run this report. The predefined IT Security Manager job role has this privilege by default.

To run the User Password Changes Audit Report:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the User Password Changes Audit Report.
4. In the **Process Details** dialog box, set parameters and click **Submit**.
5. Click **OK** to close the **Confirmation** message.

User Password Changes Audit Report Parameters

Search Type

Specify whether the report is for all users, a single, named user, or a subset of users identified by a name pattern that you specify.

User Name

Search for and select the user on whom you want to report. This field is enabled only when **Search Type** is set to **Single user**.

User Name Pattern

Enter one or more characters that appear in the user names on which you want to report. For example, you could report on all users whose user names begin with the characters **SAL** by entering **SAL%**. This field is enabled only when **Search Type** is set to **User name pattern**.

Start Date

Select the start date of the period during which password changes occurred. Changes made before this date don't appear in the report.

To Date

Select the end date of the period during which password changes occurred. Changes made after this date don't appear in the report.

Sort By

Specify how the report output is sorted. The report can be organized by either user name or the date when the password was changed.

Viewing the Report Results

The report produces these files:

- UserPasswordUpdateReport.csv
- UserPasswordUpdateReport.xml
- Diagnostics_[process ID].log

For each user whose password changed in the specified period, the report includes:

- The user name.
- The first and last names of the user.
- The user name of the person who changed the password.
- How the password was changed:
 - ADMIN means that the change was made for the user by a line manager or the IT Security manager, for example.
 - SELF_SERVICE means that the user made the change by setting preferences or requesting a password reset, for example.
 - FORGOT_PASSWORD means that the user clicked the **Forgot Password** link when signing in.
- The date and time of the change.

FAQs for Reporting on Application Users and Roles

Can I extract details of all Oracle Fusion Applications users?

Yes. The Oracle BI Publisher report User Details System Extract provides details of user accounts. For example, you can produce a report showing all user accounts, inactive user accounts, or accounts created between specified dates.

To run the report, you need a data role that provides view-all access to person records for the Human Capital Management Application Administrator job role.

How can I find out which roles a user has?

Search for and select the user on the Roles tab of the Security Console. In the visualization area, you can see the user's role hierarchy in tabular or graphical format.

Alternatively, you can run the User Role Membership Report for one or more users.

12 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 perform the Assign Security Profiles to Role task in the Setup and Maintenance work area. Alternatively, you can use the Manage Data Role and Security Profiles task. Both tasks open the Manage Data Roles and Security Profiles page. You must have the IT Security Manager job role to perform these tasks.

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, document type, and payroll flow 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 objects secured by security profiles, then you can't create an HCM data role.

 **Note:** If you create custom job roles, then the role category must end with **Job Roles**. Otherwise, they don't appear in the list of job roles when you create an HCM data role.

Security Profiles

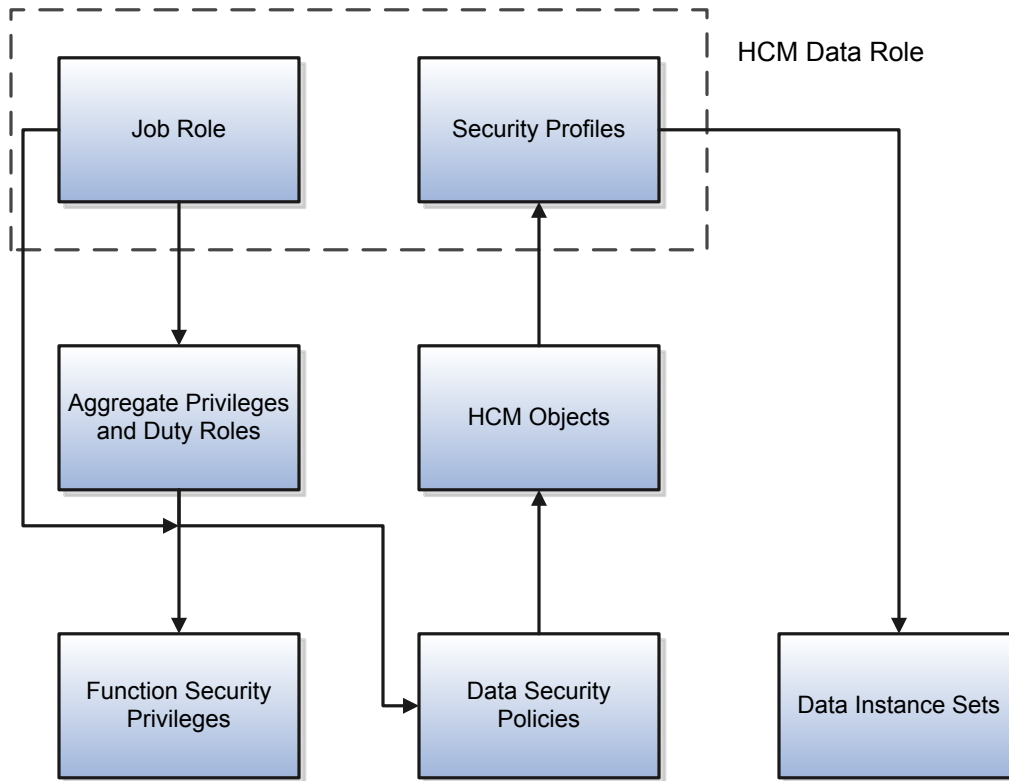
For each object type, you can include only one security profile in an HCM data role.

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 is granted many function security privileges and data security policies directly. It also inherits many aggregate privileges, and may inherit some duty roles. Each aggregate privilege or duty role has its own function security privileges and related data security policies. Relevant HCM object types are identified automatically

from the data security policies that the job role is granted either directly or indirectly. 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 Manage Work Relationship and Promote Worker aggregate privileges, among many others. The aggregate privileges provide both function security privileges, such as Manage Work Relationship and Promote Worker, and access to objects, such as assignment. Security profiles identify specific instances of those objects for the HCM data role, such as persons with assignments in a specified legal employer.

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 must have 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
- 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.

Access to Future-Dated Objects

By default, users can't access future-dated organization, position, or person objects.

To enable access to future-dated:

- Organizations, select the **Include future organizations** option in the organization security profile
- Positions, select the **Include future positions** option in the position security profile
- Person records, select the **Include future people** option in the person security profile

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 Manage Position Security Profile task in the Setup and Maintenance work area.

Security profiles that provide view-all access are predefined.

Reuse 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 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 these predefined HCM security profiles.

Security Profile Name	Security Profile Type	Data Instance Set
View All People	Person	All person records in the enterprise
View Own Record	Person	The signed-in user's own person record and the person records of that user's contacts
View Manager Hierarchy	Person	The signed-in user's line manager hierarchy
View All Workers	Person	The person records of all people with currently active or suspended assignments in the enterprise
View All Organizations	Organization	All organizations in the enterprise
View All Positions	Position	All positions in the enterprise
View All Legislative Data Groups	LDG	All LDGs in the enterprise
View All Countries	Country	All countries in the FND_ TERRITORIES table
View All Document Types	Document Type	All custom document types in the enterprise
View All Payrolls	Payroll	All payrolls in the enterprise
View All Flows	Payroll Flow	All payroll flows in the enterprise

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.

Vision Corporation is a global enterprise with multiple legal employers. Each human resource (HR) specialist in Vision Corporation has a defined area of responsibility as the human resources representative for a single legal employer. This example shows how to create a single HCM data role that you can assign to all HR specialists in Vision Corporation. This data role secures access to person records based on each HR specialist's area of responsibility.

The following table summarizes key decisions for this scenario.

Decisions to Consider	In This Example
Which job role does the HCM data role include?	Human resource specialist
Can the role be delegated?	No
Which person records do users access?	Person records of all employees, contingent workers, pending workers, and nonworkers in the legal employer for which they have the human resources representative responsibility
Which public person records do users access?	All
Which organizations do users access?	All
Which positions do users access?	All
Which countries do users see in lists of countries?	All
Which legislative data groups (LDGs) do users access?	All
Which document types do users access?	All
Which payrolls do users access?	All
Which payroll flows do users access?	All

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 any new security profiles

4. Reviewing and submitting the HCM data role

Prerequisites

Before you can perform these tasks:

1. Human resources representatives must have been identified for each legal employer.
2. An area of responsibility must have been created for each human resources representative. The **Responsibility Type** is set to **Human resources representative**, and the scope of responsibility is set to the relevant legal employer.

Naming the HCM Data Role and Selecting the Job Role

1. Select **Navigator - Setup and Maintenance**.
2. In the Setup and Maintenance work area, search for and select the Assign Security Profiles to Role 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.

Field	Value
Data Role	Legal Employer HR Specialist
Job Role	Human Resource Specialist
Delegation Allowed	No

5. Click **Next**.

Specifying Security Criteria for Each HCM Object Type

1. In the Organization section of the Create Data Role: Security Criteria page, select the predefined organization security profile View All Organizations.
2. In the Position section, select the predefined position security profile View All Positions.
3. In the Countries section, select the predefined country security profile View All Countries.
4. In the Legislative Data Group section, select the predefined LDG security profile View All Legislative Data Groups.
5. In the Person section, complete the fields as shown in the table.

Field	Value
Person Security Profile	Create New
Name	Workers by Legal Employer
Secure by Area of Responsibility	Yes

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 predefined payroll security profile View All Payrolls.
9. In the Payroll Flow section, select the predefined payroll flow security profile View All Flows.
10. Click **Next** until you reach the Assign Security Profiles to Role: Person Security Profile page.

Creating the Person Security Profile

1. In the Area of Responsibility section, ensure that the **Secure by area of responsibility** option is selected.
2. Complete the fields as shown in this table.

Field	Value
Responsibility Type	Human resources representative
Scope of Responsibility	Legal employer

3. Click **Review**.

Review and Submit the HCM Data Role

1. 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 helps minimize maintenance and eases their introduction in your enterprise. This topic suggests some approaches.

Minimizing Numbers of Data Roles and Security Profiles

Secure access to person records based on a user's areas of responsibility whenever possible. Using this approach, you can:

- Reduce dramatically the number of HCM data roles and security profiles that you must manage.
- Avoid the performance problems that can occur with large numbers of HCM data roles.

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 organizations in a single country. If you create an organization security profile that provides this access, 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 position security profile name All Positions Sales Department conveys that the security profile identifies all positions 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 Specialist Legal Employer identifies both the job role and the role scope. HCM data role names must contain fewer 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 both legal employers and departments, then the organization security profile 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.

Auditing Changes to HCM Data Roles and Security Profiles

A user with the Application Implementation Consultant job role can enable audit of changes to HCM data roles and security profiles for the enterprise.

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 - About Me - 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 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 worker directory.

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 gains 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, 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.

Delegation from Multiple Delegators


Multiple users can delegate the same role to the same proxy for overlapping periods. If the proxy user already has the role, then it isn't provisioned again but the proxy can access the data associated with the delegated roles. For example, three line managers delegate the line manager role to the same proxy for the following periods:

- Manager 1, January and February
- Manager 2, February and March
- Manager 3, January through April

This table shows which manager hierarchies the proxy can access in each month.

January	February	March	April
Manager 1	Manager 1		
	Manager 2	Manager 2	
Manager 3	Manager 3	Manager 3	Manager 3

If the proxy is a line manager, then the proxy can access his or her own manager hierarchy in addition to those from other managers.

 **Note:** A single delegator can't delegate the same role to the same proxy more than once for overlapping periods.

Role Delegation Dates

You can enter both start and end dates or a start date only.

- If the start date is today's date, then the delegation is immediate.
- If the start and end dates are the same, then the delegation is immediate on the start date. A request to end the delegation is generated on the same date and processed when the Send Pending LDAP Requests process next runs.
- If the start and end dates are different and in the future, then requests to start and end delegation are generated on the relevant dates. They're processed when Send Pending LDAP Requests runs on those dates.
- If you change a delegation date to today's date, then the change is immediate if the start and end dates are different. If they're the same, then a request to end the delegation is generated and processed when Send Pending LDAP Requests next runs.
- If you enter no end date, then the delegation is indefinite.

Role delegation ends automatically if the proxy user's assignment is terminated.

Enabling Role Delegation: Explained


By default, delegation isn't enabled for any predefined HCM job or abstract role. You can change the delegation setting of any predefined HCM role, except the Employee and Contingent Worker abstract roles. You can also enable delegation for HCM data roles, custom job roles, and custom abstract roles.

This topic describes how to manage role delegation using the Assign Security Profiles to Role task in the Setup and Maintenance work area. You must have the IT Security Manager job role to manage role delegation.

Delegation of HCM Data Roles


When you create an HCM data role, you can indicate whether delegation is allowed on the Create Data Role: Select Role page.

When you edit an HCM data role, you can change the delegation setting on the Edit Data Role: Role Details page. If you deselect the **Delegation Allowed** option, then currently delegated roles aren't affected.

 **Note:** You can delegate HCM data roles in which access to person records is managed using custom criteria. However, the SQL predicate in the Custom Criteria section of the person security profile must handle the delegation logic.

Delegation of Custom Job and Abstract Roles

If you create a custom abstract role, then you can enable it for delegation when you assign security profiles to it directly. To assign security profiles to abstract roles, you perform the Assign Security Profiles to Role task. On the Edit Data Role: Role Details page, you select **Delegation Allowed**. As soon as you submit the role, delegation is enabled.

 **Note:** You can't delegate access to your own record. For example, you may assign the predefined View Own Record security profile to your custom role. Alternatively, you may create a person security profile that enables access to your own record and assign it to your custom role. In both cases, you can enable the role for delegation. Although the role itself can be delegated, access to your record isn't delegated. However, the delegated role can provide access to other data instances.

You can enable custom job roles for delegation in the same way, but you're unlikely to assign security profiles to them directly. Typically, job roles are inherited by HCM data roles, which you can enable for delegation.

Assigning Security Profiles to Job and Abstract Roles: Procedure

To give users access to data you usually create HCM data roles, which inherit job roles. However, you can also assign security profiles directly to job and abstract roles. You're most likely to assign security profiles to abstract roles, such as employee, to provide the data access that all employees need. For example, all employees must be able to access the worker directory. You're less likely to assign security profiles to job roles, as users with the same job role typically access different data instances.


This topic describes how to:

- Assign security profiles directly to a job or abstract role.
- Remove security profiles from a job or abstract role.

Assigning Security Profiles to Roles

You can assign security profiles to both predefined and custom job and abstract roles. Follow these steps to assign security profiles to a role:


1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Assign Security Profiles to Role task.
3. On the Manage Data Roles and Security Profiles page, search for the job or abstract role.
4. In the search results, select the role and click **Edit**.
5. On the Edit Data Role: Role Details page, click **Next**.
6. On the Edit Data Role: Security Criteria page, select the security profiles that you want to assign to the role.
7. Click **Review**.
8. On the Edit Data Role: Review page, click **Submit**.

 **Tip:** On the Manage Data Roles and Security Profiles page, search for the role again. In the search results, confirm that a green check mark appears in the **Security Profiles Assigned** column. The check mark confirms that security profiles are assigned to the role.

Revoking Security Profiles from Roles

You can remove security profiles that you assigned directly to a predefined or custom abstract or job role. For example, you may have assigned security profiles directly to a job role and included the job role in a data role later. In this case, users may have access to more data than you intended. Follow these steps to remove security profiles from a role:

1. On the Manage Data Role and Security Profiles page, search for the job or abstract role.
2. In the search results, select the role and confirm that security profiles are currently assigned to the role.
3. Click **Revoke Security Profiles**. All security profiles currently assigned directly to the role are revoked.

 **Note:** To replace the security profiles in an HCM data role, edit the data role in the usual way. You can't use the **Revoke Security Profiles** button.

Configuring HCM Data Roles and Security Profiles for Audit: Procedure

This procedure describes how to configure the attributes of HCM data roles and security profiles for audit. You must have the Application Implementation Consultant job role to perform this task.

1. Select **Navigator - Setup and Maintenance**.
2. Search for and select the **Manage Audit Policies** task.
3. On the Manage Audit Policies page, click **Configure Business Object Attributes** in the Oracle Fusion Applications section.
4. On the Configure Business Object Attributes page, set **Application** to **HCM Core Setup**.
5. In the **Audit** column of the table of business objects that appears, select an object. For example, select **Person Security Profile** or **Data Role**.
6. In the Audited Attributes section of the page, click **Create**.

The **Select and Add Audit Attributes** dialog box opens.
7. In the **Select and Add Audit Attributes** dialog box, select one or more attributes for audit and click **OK**.
8. Click **Save and Close**.
9. On the Manage Audit Policies page, set **Audit Level** to **Auditing** in the Oracle Fusion Applications section.
10. Click **Save and Close**.

Changes made from now on to the selected attributes of the object are audited. A user who has the Internal Auditor job role can review audited changes on the Audit Reports page.

Related Topics

- [Managing Audit Policies: Explained](#)
- [Configuring Audit Business Object Attributes: Points to Consider](#)

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.

Create Custom 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. To enable this access, you create a custom version of the job role to which you add the relevant privileges. You include the custom job role in an HCM data role with one or more security profiles that identify the data.

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 Diagnostics 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 Diagnostics 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 Diagnostics Tests**.

Diagnostic Test Parameters

Securing Object

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

Securing Object Name	Description
PERSON	Person
LDG	Legislative data group
POSITION	Position
ORGANIZATION	Organization
PAYROLL	Payroll
FLOWPATTERN	Payroll flow
DOR	Document type
COUNTRY	Country

If you don't enter the name of a securing object, then the test applies to all securing objects.

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, then 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.

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

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

Diagnostic Test Name	Tests
HCM Data Roles Configuration	Configuration of Manage HCM Data Roles for a user
HCM Data Role Detailed Information	Potential problems with a data role

Diagnostic Test Name	Tests
HCM Security Profile Configuration	Configuration of Manage Security Profiles tasks for a user
HCM Security Profiles Detailed Information	Potential problems with security profiles of a type
HCM Securing Objects Metadata	Securing-object metadata

13 Person Security Profiles

Securing Person Records: Points to Consider

This topic describes ways of securing access to both public and managed person records. The recommended approaches minimize administration and improve security performance.

Securing Public Person Records

Public person records are those that all workers must access in a worker directory, for example. Use the View All Workers predefined security profile to provide this access. View All Workers provides access to:

- Employees, contingent workers, nonworkers, and pending workers
- The signed-in user's own record
- Shared person information

View All Workers doesn't provide access to future person records.

Securing Person Records by Manager Hierarchy

Managers must access the person records of the workers in their manager hierarchies. To provide this access, you secure person records by manager hierarchy. Use the predefined View Manager Hierarchy security profile wherever possible. This table summarizes the View Manager Hierarchy security profile. The values shown here are also the default values for these fields.

Field	Value
Person or Assignment Level	Person
Maximum Levels in Hierarchy	No maximum
Manager Type	Line Manager
Hierarchy Content	Manager Hierarchy

View Manager Hierarchy includes shared person information but not future person records.

For nonstandard requirements, create custom person security profiles. For example, if your enterprise has a custom Project Manager job role, then you can create a security profile for that manager type. Include it in an HCM data role and provision that role to all users who have the Project Manager job role.

Securing Person Records by Area of Responsibility

When you secure person records by area of responsibility, the set of records that a user can access is calculated dynamically. The calculation is based on the user's assigned areas of responsibility. This approach has several advantages:

- It reduces the number of person security profiles and HCM data roles that you must manage.
- It improves security performance.
- You don't have to update security profiles when responsibilities change.

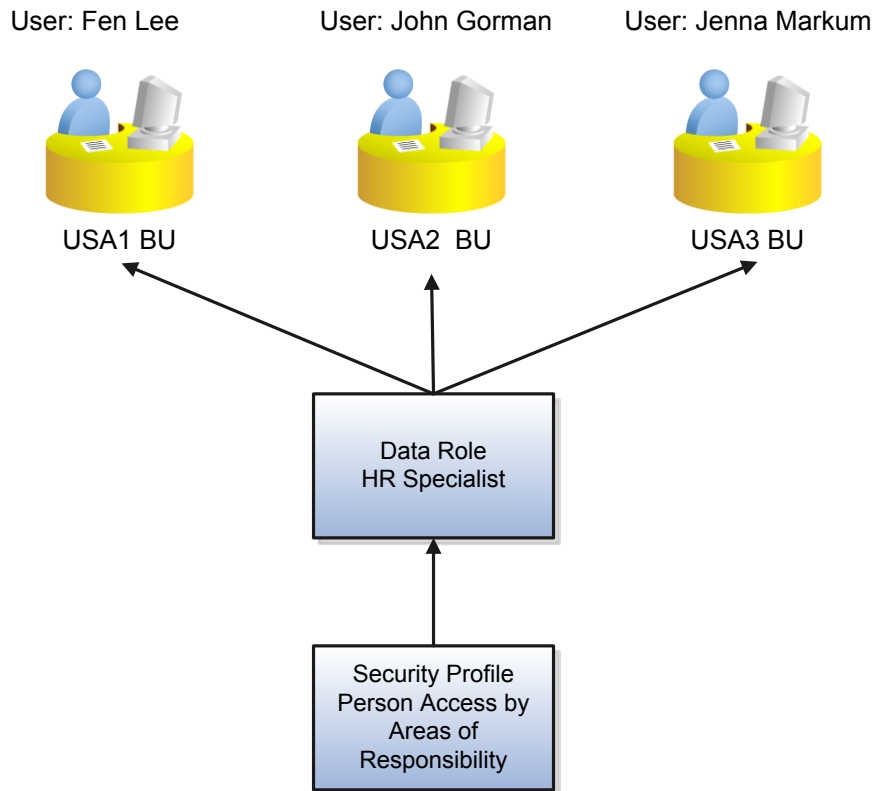
For example, consider these human resource (HR) specialists, who perform the same job role but for workers in different business units:

HR Specialist	Job Role	Business Unit
Fen Lee	Human Resource Specialist	USA1 BU
John Gorman	Human Resource Specialist	USA2 BU
Jenna Markum	Human Resource Specialist	USA3 BU

To provide access to person records in each business unit, you:

- Define an area of responsibility for each HR specialist, where the scope of responsibility is the relevant business unit.
- Create a single person security profile that restricts access by area of responsibility and where **Scope of Responsibility** is **Business unit**.
- Create a single HCM data role to include the person security profile and assign it to all three HR specialists.

This figure summarizes the approach.



Tip: Scope of responsibility in a person security profile can be any one of several values, such as department or payroll. For users, define areas of responsibility based on a single scope value that you can also select in a person security profile.

When you secure access to person records by area of responsibility, the user doesn't see all of the worker's assignments. Instead:

- For current workers, authorized users can see current and suspended assignments only. Access to terminated assignments, such as those that were active before a global transfer, is prevented.
- For terminated workers, authorized users can see the most recently terminated assignment only.

Securing Access to Imported Candidates

You can secure access to the records of candidates imported from Oracle Taleo Recruiting Cloud Service. Set the **Purpose** field in the Basic Details section of the person security profile to one of these values:

- Imported Candidate Access
- Person and Imported Candidate Access

You can secure access to imported candidates by either area of responsibility or manager hierarchy.

The **Purpose** field is available only if the **Recruiting Integration** enterprise option is set to one of these values:

- Integrated with HCM Connect
- Fixed and Integrated with HCM Connect

Otherwise, the **Purpose** field doesn't appear.


Securing Person Records by Area of Responsibility: Procedure

In most cases, you secure access to person records by either manager hierarchy or area of responsibility. To secure by area of responsibility, you must first define areas of responsibility for relevant workers. This topic describes how to create a person security profile where access is secured by area of responsibility.

Defining the Person Security Profile

Follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the **Manage Person Security Profile** task.
3. On the Manage Person Security Profiles page, click **Create**.
4. In the Basic Details section of the Create Person Security Profile page, enter a name for the security profile. Complete other fields in the Basic Details section, as appropriate.
5. In the Area of Responsibility section, select **Secure by area of responsibility**.
6. Select a **Responsibility Type** value. For example, select **Benefits representative** or **Union representative**.
7. Select a **Scope of Responsibility** value. For example, if you select **Legal Employer**, then users can access person records in the legal employer for which they have the selected **Responsibility Type**.


 **Note:** An area of responsibility can be based on multiple scope values, for example, both legal employer and job. In this case, only one of those values must be matched by the security profile.

8. All worker types are selected by default. Deselect any that don't apply.
9. Click **Next**.

Previewing the Person Security Profile

On the Create Person Security Profile: Preview page, you can test the access that your security profile provides before you save it. Follow these steps:

1. On the Person Access Preview tab, select a user and click **Preview**. Typically, you select a user who has the area of responsibility that you identified when defining the security profile.
 - The User Summary section of the page is updated automatically to show the number of person records that this user could access.
 - The Assigned Areas of Responsibility section of the tab shows the selected user's areas of responsibility.

 **Note:** The results from the Person Access Preview are based on the current person security profile only. Users may have roles that provide access to other person records.


2. In the Search Person section of the tab, you can search for specific person records to which the security profile provides access. The search is within the set of person records that was identified when you clicked **Preview** for the named user. For example, if the preview identified 50 person records, then the search is of those 50 person records.
3. To view the SQL predicate generated by this security profile, click the SQL Predicate for Person Access tab.
4. Click **Save and Close** to save the security profile.

Related Topics

- [Areas of Responsibility: Explained](#)
- [Setting Scope of Responsibility: Examples](#)

Securing Person Records by Manager Hierarchy: Points to Consider

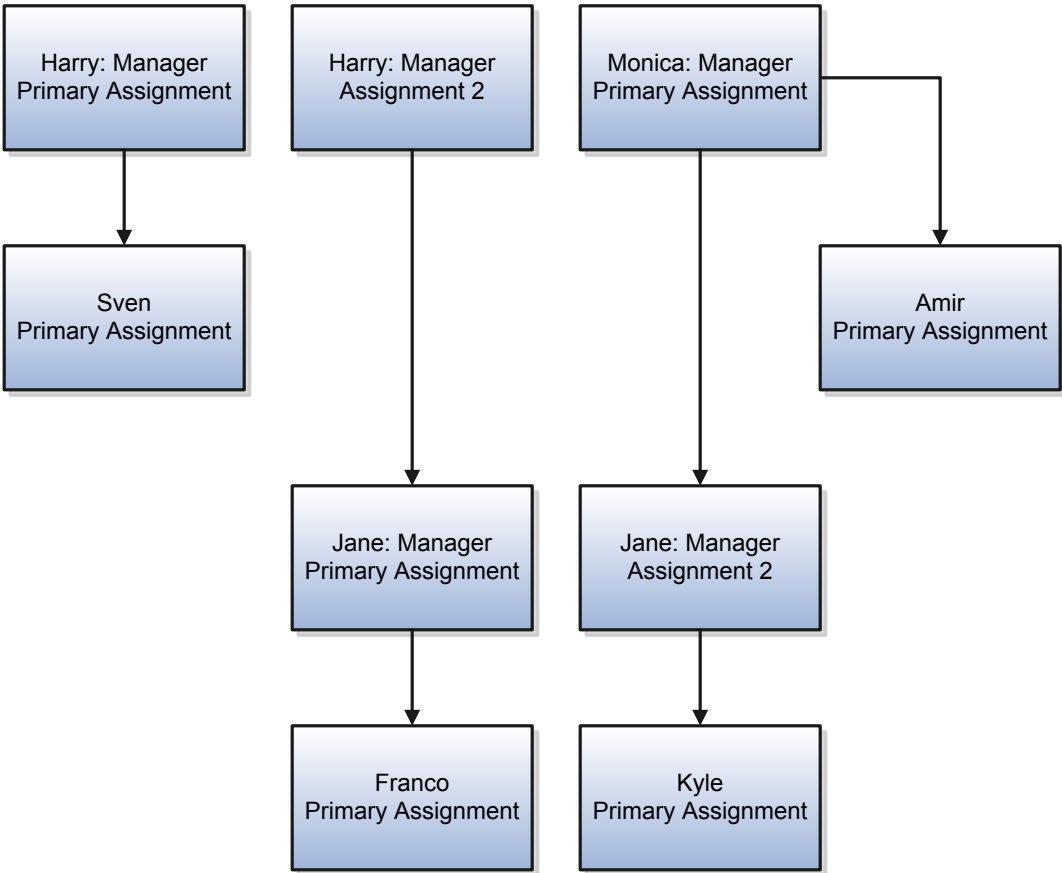
The person records that a manager can access depend on how you specify the manager hierarchy in the person security profile. This topic describes the effect of the **Person or Assignment Level** option, which you set to either **Person** or **Assignment**.


 **Note:** The **Person or Assignment Level** option, regardless of its setting, controls access to person records. You can't enable access to particular assignments.

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.



 **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.

Person-Level Manager Hierarchy

When **Person or Assignment Level** is **Person**, the security profile includes any person reporting directly or indirectly to any of the manager's assignments.

This table shows the person records that each of the three managers can access in a person-level manager hierarchy.

Manager	Sven	Jane	Franco	Kyle	Amir
Harry	Yes	Yes	Yes	Yes	
Monica		Yes	Yes	Yes	Yes
Jane			Yes	Yes	

Manager	Sven	Jane	Franco	Kyle	Amir
---------	------	------	--------	------	------

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. For example, Harry can access Kyle's person record, even though Kyle doesn't report to an assignment that Harry's manages.

Assignment-Level Manager Hierarchy

When **Person or Assignment Level** is **Assignment**, managers see the person records of people who:

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

Manager	Sven	Jane	Franco	Kyle	Amir
Harry	Yes	Yes	Yes		
Monica		Yes		Yes	Yes
Jane			Yes	Yes	

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.

Related Topics

- [The Manager Hierarchy: How It's Maintained](#)

Specifying the Manager Type: Explained

When you secure person records by manager hierarchy, the security profile's data instance set includes 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.

This table describes the **Manager Type** values.

Manager Type	Description
All	The security profile includes all types of manager hierarchies.
Line Manager	The security profile includes only the line manager hierarchy.
Selected	The security profile includes only the specified type of manager hierarchy.

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 by selecting **Navigators - My Team**, for example.

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 **Navigators - Setup and Maintenance** to open the Setup and Maintenance work area and search for the Manage Person Security Profile task.


Hierarchy Content Values

This table describes the **Hierarchy Content** values.

Value	Description
Manager hierarchy	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.
Delegating manager hierarchy	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.
Both	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.

Value	Description
-------	-------------

When the line manager role is delegated to another line manager, the proxy can manage the delegator's reports in the Person Management work area and Directory. However, the proxy's My Team information 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 Using Custom Criteria: Examples

You can secure person records by either area of responsibility or manager hierarchy. 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 SQL 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.

Identifying Persons Born Before a Specified Date

This scenario shows how to use custom criteria in a person security profile. The person security profile data instance set must include persons who were born before 01 January, 1990.


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

```
&TABLE_ALIAS.PERSON_ID IN (SELECT PERSON_ID FROM PER_PERSONS
WHERE DATE_OF_BIRTH < TO_DATE('01-JAN-1990', 'DD-MON-YYYY'))
```

Defining Exceptions to Areas of Responsibility

You may want to exclude some worker records from the data instance set defined by an area of responsibility. For example, a worker may have access to all workers in an organization, except those in specific grades or locations. In these cases, you use custom criteria.

In very simple cases, you can use both the Area of Responsibility and Custom Criteria sections of the person security profile. You use the custom criteria to define just the exceptions in addition to any criteria specified in the Area of Responsibility section. More typically, especially where the exclusion is based on assignment values, you are recommended to use only the Custom Criteria section. This approach is recommended for performance reasons.

 **Tip:** Use the Area of Responsibility section temporarily to define the basic access. Copy the SQL predicate from the SQL Predicate for Person Access tab on the Create Person Security Profile: Preview page to use as the basis of your custom criteria.

Tables and Views in Custom Criteria: Explained

You can secure access to person records using custom criteria in the form of SQL predicates. This topic identifies tables and views that you can't use in custom SQL statements. The use of any of these tables or views is likely to cause errors, where the error message contains the text **ORA28113: POLICY PREDICATE HAS ERROR**.

This table identifies tables and views that you must not include in custom SQL statements when securing access to person records.

Product	Table or View
Contracts	<ul style="list-style-type: none"> OKC_EMPLOYEE_CONTACT_V OKC_SEARCH_EMPLOYEE_V OKC_SEARCH_INT_CONTACTS_V OKC_SIGNER_CONTACTS_V
Financials for EMEA	<ul style="list-style-type: none"> JE_RU_FA_EMPLOYEE_V
General Ledger	<ul style="list-style-type: none"> GL_HIERVIEW_PERSON_INFO_V
Global Human Resources	<ul style="list-style-type: none"> HR_BU_LOCATIONS_X HR_LOCATIONS HR_LOCATIONS_ALL HR_LOCATIONS_ALL_F HR_LOCATIONS_ALL_F_VL HR_LOCATIONS_ALL_VL HR_LOCATIONS_ALL_X PER_ADDRESSES_F PER_ADDRESSES_FU_SEC PER_ADDRESSES_F_ PER_ADDRESSES_F_SEC PER_CONT_WORKERS_CURRENT_X PER_CONT_WORKERS_X PER_DISPLAY_PHONES_V PER_DRIVERS_LICENSES PER_DRIVERS_LICENSESU_SEC PER_DRIVERS_LICENSES_ PER_DRIVERS_LICENSES_SEC PER_EMAIL_ADDRESSES PER_EMAIL_ADDRESSESU_SEC PER_EMAIL_ADDRESSES_ PER_EMAIL_ADDRESSES_SEC PER_EMAIL_ADDRESSES_V PER_EMPLOYEES_CURRENT_X PER_EMPLOYEES_X PER_LOC_OTHER_ADDRESSES_V PER_NATIONAL_IDENTIFIERS PER_NATIONAL_IDENTIFIERSU_SEC PER_NATIONAL_IDENTIFIERS_ PER_NATIONAL_IDENTIFIERS_SEC

Product	Table or View
	<ul style="list-style-type: none"> • PER_NATIONAL_IDENTIFIERS_V • PER_PASSPORTS • PER_PASSPORTSU_SEC • PER_PASSPORTS_ • PER_PASSPORTS_SEC • PER_PERSON_ADDRESSES_V • PER_PHONES • PER_PHONESU_SEC • PER_PHONES_ • PER_PHONES_SEC • PER_PHONES_V • PER_VISAS_PERMITS_F • PER_VISAS_PERMITS_FU_SEC • PER_VISAS_PERMITS_F_SEC • PER_WORKFORCE_CURRENT_X • PER_WORKFORCE_X
Global Payroll	<ul style="list-style-type: none"> • PAY_AMER_W4_LOC_ADDRESS_V • PAY_AMER_W4_PERSON_ADDRESS_V
Grants Management	<ul style="list-style-type: none"> • GMS_ALL_CONTACTS_V • GMS_INTERNAL_CONTACTS_V
Payments	<ul style="list-style-type: none"> • IBY_EXT_FD_EMP_HOME_ADDR
Planning Common Components	<ul style="list-style-type: none"> • MSC_AP_INTERNAL_LOCATIONS_V
Profile Management	<ul style="list-style-type: none"> • HRT_PERSONS_D • HRT_PERSONS_X
Project Foundation	<ul style="list-style-type: none"> • PJF_PROJ_ALL_MEMBERS_V • PRJ_PROJECT_MANAGER_V • PRJ_TEAM_MEMBERS_F_V
Workforce Reputation Management	<ul style="list-style-type: none"> • HWR_VLTR_REGN_RGSTR_VL • HWR_VLTR_REGN_TOTAL_VL

For more information about tables and views, see the Tables and Views for Oracle HCM Cloud guide.

FAQs for Person Security Profiles

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

Users who see the Contacts tab in the Manage Person work area can see a worker's contacts, unless the contacts are workers. If a contact is a worker, then the contact's details are secured by person security profile. Personally identifiable information (PII), such as phones and e-mails, isn't visible unless the user inherits the Manage Contact Person PII aggregate privilege.

Any user can see the contact records of his or her own contacts.

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, regardless of the assignment type. The assignments can also be with different legal employers.

What happens if I include shared information in a person security profile?

Users can access any person information that's shared with them. This access is in addition to the person records identified by the person security profile. If you leave this option deselected, then users can't access shared person information unless the shared person record is identified by the person security profile.

What happens if I include future objects in a security profile?

Users can access future-dated persons, organizations, or positions that satisfy the security profile criteria. If you leave this option deselected, then users can't access future-dated objects. For example, users couldn't see an organization with a future start date, even though it satisfied all other criteria in the security profile.

Date-effective records in objects aren't affected by this option.

Can I secure access to person records by workforce structures or global name range?

Yes, but only if you upgraded from Release 11. If your implementation was new in Release 12 or later, then you can't secure access to person records by workforce structures or global name range.

14 Organization and Other Security Profiles

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.

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

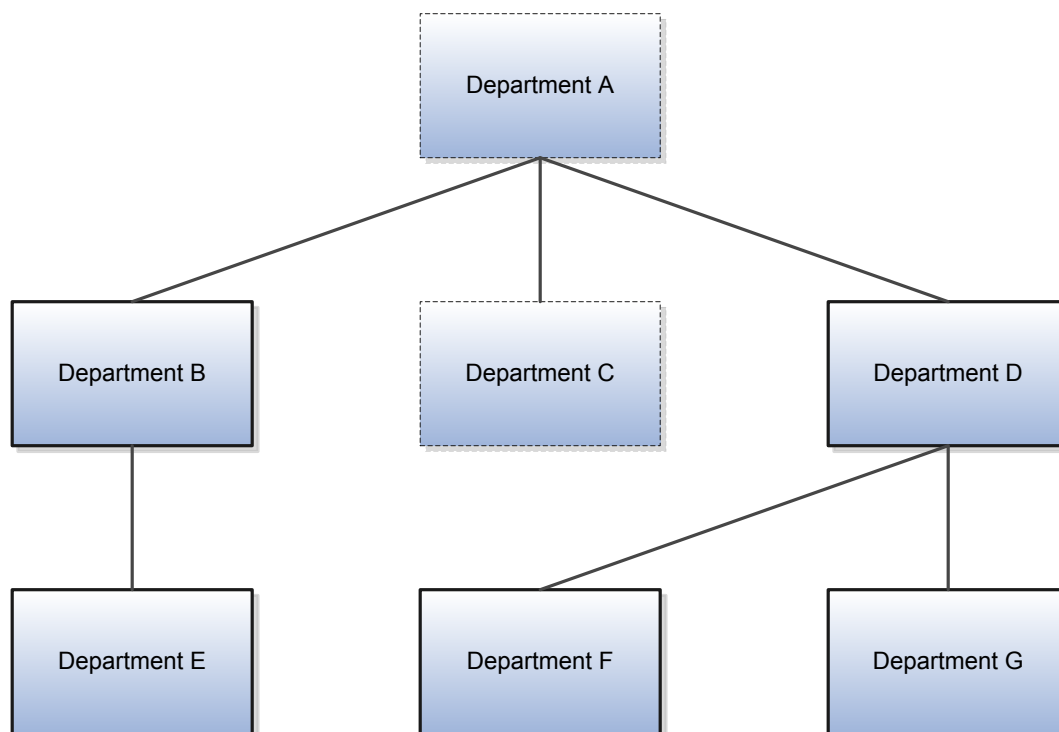
If you select a named organization as the top organization in an organization hierarchy, then you must ensure that the organization remains valid. No automatic validation of the organization occurs, because changes to the organization hierarchy occur independently of the organization security profile.

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 departments 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 department B and one in department D, which belong to the same organization hierarchy. The top organizations are departments B and D, and the user's data instance set of organizations therefore includes departments 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.

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 by editing their personal information. 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 for 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 Profile* task in the Setup and Maintenance work area.

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.

Creating Payroll Security Profiles: Examples

These examples illustrate different methods you can use to provide access to payrolls for members of the Payroll department. You first organize your payroll definitions into appropriate payroll security profiles using the *Manage Payroll Security Profiles* task. Then you use the *Assign Security Profiles to Role* task to select the security profiles included in an HCM data role that you provision to a user.

Payroll Period Type

Using a payroll security profile to organize payroll definitions by payroll period type is the most common example. You create one security profile for monthly payrolls, another for semimonthly payrolls, and so on.

Regional Assignments

You can use payroll security profiles to group payrolls by the regions of the target employees' work areas. For example, you can create one for Canadian facilities and another for European facilities.

Individual Contributors

Your company requires that payroll managers access only the payroll definitions that they manage. In this scenario, the payroll security profile includes only those payrolls.

Creating Flow Pattern Security Profiles: Examples

The following examples illustrate different methods you can use to organize payroll flows into appropriate security profiles. Use the Assign Security Profiles to Role task in the Setup and Maintenance work area to grant workers access to those profiles by data role.

Payroll Processing and QuickPay Flows

Payroll administrators are responsible for payroll processing. The payroll flow security profiles for the payroll administrator data role include the Payroll Cycle flow and the QuickPay flow.

End of Year Reporting

Some payroll administrators are responsible for year-end reporting. The payroll flow security profiles for their data role includes the End of Year flow and the Archive End-of-Year Payroll Results flow.

Hiring and Terminations

HR administrators are responsible for hiring and terminating employees. The payroll flow security profiles for the HR specialist data role includes the New Hire flow and the Termination flow.

Flow Security and Flow Owners: Explained

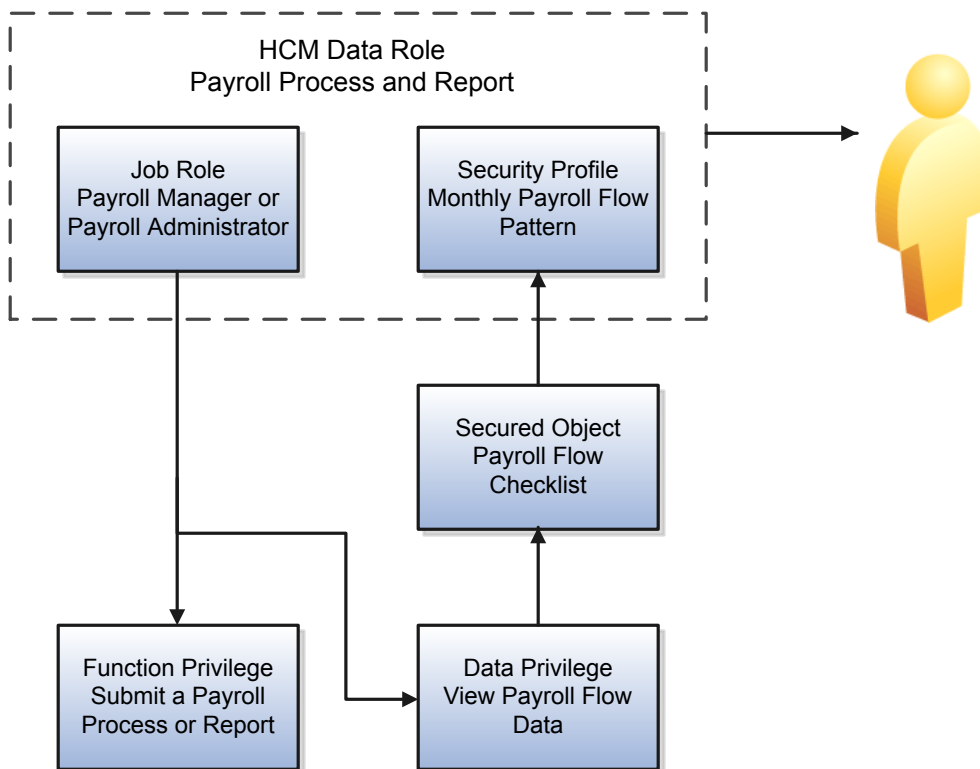
Your HCM data role security determines which flows you can submit or view. This topic explains how the HCM data roles and flow security work together. You define security for flow patterns using the Manage Payroll Flow Security Profile task in the Setup and Maintenance work area.

Submitting a flow generates a checklist of the included tasks. You become the owner of the flow and its tasks. If a flow pattern designates tasks to different owners, you remain the flow owner. Either you or the owner of a task can reassign the task to someone else, for example, to cover situations where the task is overdue and the task owner is on leave.

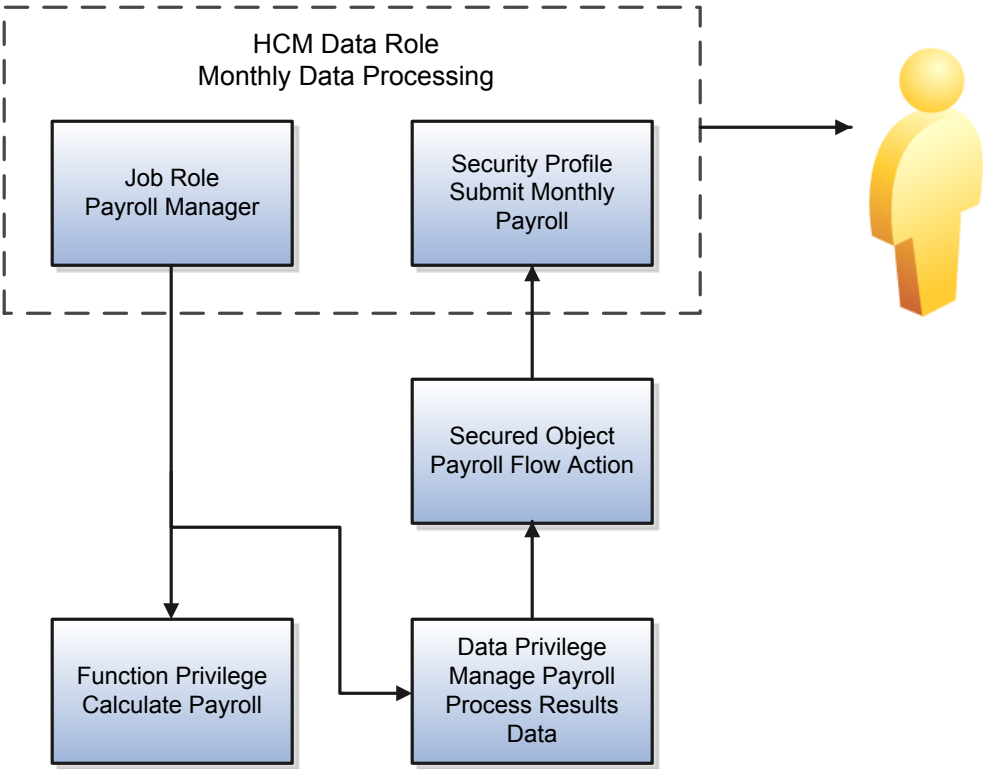
Payroll Flow Security and HCM Data Roles

HCM data roles secure the access to flows through data privileges and to the tasks on a checklist through functional privileges.

The following figure illustrates how the payroll manager and payroll administrator can submit a process or report and can view the results of the monthly payroll flow. Either the payroll manager or the payroll administrator can submit the flow and perform its tasks or have the tasks reassigned to them.



The following figure illustrates how only the payroll manager can calculate the payroll. The payroll manager can't reassign this task to a payroll administrator, because the administrator doesn't have the necessary functional privileges.



Troubleshooting

The following table describes what action to take if you encounter problems submitting or completing a task in a flow.

Problem	Solution
Can't submit or view a flow	Confirm that the data role assigned to you includes a security profile for the payroll flow pattern.
Can't perform a task, such as a process or report	Confirm that your data role is based on a job or abstract role that includes functional privileges to perform that task.

Related Topics

- [Checklist and Flow Tasks: Explained](#)
- [Flow Pattern Parameters: Explained](#)

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.

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.

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.

What happens if I include future objects in a security profile?

Users can access future-dated persons, organizations, or positions that satisfy the security profile criteria. If you leave this option deselected, then users can't access future-dated objects. For example, users couldn't see an organization with a future start date, even though it satisfied all other criteria in the security profile.

Date-effective records in objects aren't affected by this option.

15 Using the Security Console

Graphical and Tabular Role Visualizations: Explained

On the Roles tab, you can review role hierarchies. You see either a tabular or a graphical view of a role hierarchy. Which view you see by default depends on the setting of the **Enable default table view** option on the Administration tab. This topic describes how to use each of these views.

Role hierarchies stretch from users at the top of the hierarchy to privileges at the bottom. In both graphical and tabular views, you can set the direction of the displayed hierarchy.

- To show from the selected user, role, or privilege up the hierarchy, set **Expand Toward** to **Users**.
- To show from the selected user, role, or privilege down the hierarchy, set **Expand Toward** to **Roles**.

The Tabular View

If the tabular view doesn't appear when you select a security artifact on the Roles tab, then you can click the **View as Table** icon. In the tabular view, you can:

- Review the complete role hierarchy for a selected user or role. The table shows roles inherited both directly and indirectly.
- Search for a security artifact by entering a search term in the field above any column and pressing **Enter**.
- Set the contents of the table as follows:
 - If **Expand Toward** is set to **Privileges**, then you can set **Show** to either **Privileges** or **Roles**.
 - If **Expand Toward** is set to **Users**, then you can set **Show** to either **Roles** or **Users**.

The resulting contents of the table depend on the start point. For example, if you select a privilege, **Expand Toward** is set to **Privileges**, and **Show** is set to **Roles**, then the table is empty.

- Export the displayed details to a Microsoft Excel spreadsheet.

The Graphical View

If the graphical view doesn't appear when you select a security artifact on the Roles tab, then you can click the **Show Graph** icon. In the graphical view, users, privileges, and the various types of roles are represented by nodes and differentiated by both color and labels. These values are defined in the Legend. You can:

- Review roles inherited directly by the selected role or user. To see roles and privileges inherited indirectly, select a directly inherited role, right-click, and select either **Expand** or **Expand All**. Select **Collapse** or **Collapse All** to reverse the action. Alternatively, double-click a node to expand or collapse it.
- Use the **Set as Focus** action to make any selected node the center of the visualization.
- Use the Overview in the bottom right of the display area to manipulate the visualization. For example, clicking a node in the Overview moves the node to the center of the visualization. You can also use drag and drop.
- Hover on a Legend entry to highlight the corresponding nodes in the visualization. Click a legend entry to add or remove corresponding nodes in the visualization.

In the Control Panel, you can:

- Switch the layout between radial and layered representations.
- Click the **Search** icon and enter a search term to find a security artifact among currently displayed nodes.
- Zoom in and out using either the **Zoom in** and **Zoom out** icons or the mouse wheel.
- Magnify areas of the visualization by clicking the **Magnify** icon and dragging it to the area of interest. Click the icon again to switch it off.
- Click the **Zoom to Fit** icon to center the image and fill the display area

Simulating Navigator Menus: Procedure

You can simulate the Navigator for both users and roles. This feature can help you to identify how access is provided to specific work areas and tasks. You may need this information when creating custom roles, for example. This topic provides instructions for simulating the Navigator.

Simulating the Navigator for a Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the role, which can be of any type.
2. In the search results, select **Simulate Navigator** in the Actions menu for the role. The Simulate Navigator page opens. Icons may appear against Navigator entries. In particular:
 - The **Lock** icon indicates that the role can't access the entry.
 - The **Warning** icon indicates that the role may not appear in the Navigator as the result of customization, for example.

Entries without either of these two icons are available to the role.

 **Tip:** To view just the entries that the role can access, set **Show** to **Access granted**.

Viewing Roles That Grant Access to a Navigator Entry

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the roles that grant access. Follow these steps:

1. Click the entry.
2. Select **View Roles That Grant Access**.
3. In the **Roles That Grant Access** dialog box, review the list of roles. The roles can be of all types. After reviewing this list, you can decide how to enable this access, if appropriate. For example, you may decide to provision an abstract role to a user or add an aggregate privilege to a custom role.
4. Click **OK** to close the **Roles That Grant Access** dialog box.

Viewing Privileges Required for Menu

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the privileges that grant access to:

- The Navigator entry

- Tasks in the associated work area

Follow these steps:

1. Click the entry.
2. Select **View Privileges Required for Menu**.
3. In the **View Privileges for Work Area Access** dialog box, review the list of privileges that grant access to:
 - The Navigator menu item
 - Task Panel entries in the associated work area. In the **Access Granted** column of this table, you can see whether the selected role can access these tasks.

You can use this information when customizing roles, for example. You can identify how to both add and remove access to specific tasks and work areas.

4. Click **OK** to close the **View Privileges for Work Area Access** dialog box.
5. Click **Close** to close the Simulate Navigator page.

Simulating the Navigator for a User

Search for the user on the Roles tab of the Security Console and select **Simulate Navigator** in the Actions menu for the user. Follow the instructions for simulating the Navigator for a role.

Reviewing Role Assignments: Procedure

You can use the Security Console to:

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

You must have the IT Security Manager job role to perform these tasks.

Viewing the Roles Assigned to a User

Follow these steps:

1. Select **Navigator - Tools - Security Console**.
2. On the Security Console, search for and select the user.

Depending on the enterprise setting, either a table or a graphical representation of the user's role hierarchy appears. Switch to the graphical representation if necessary to see the user and any roles that the user inherits directly. User and role names appear on hover. To expand an inherited role:


1. Select the role and right-click.
2. Select **Expand**. Repeat these steps as required to move down the hierarchy.

 **Tip:** Switch to the table to see the complete role hierarchy at once. You can export the details to Microsoft Excel from here.

Identifying Users Who Have a Specific Role

Follow these steps:

1. On the Security Console, search for and select the role.
2. Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn't appear by default.
3. Set **Expand Toward** to **Users**.


 **Tip:** Set the **Expand Toward** option to control the direction of the graph. You can move either up the hierarchy from the selected role (toward users) or down the hierarchy from the selected role (toward privileges).

In the refreshed graph, blue diamond shapes identify users. User names appear on hover. Users may inherit roles either directly or indirectly from other roles, which appear as green circles. Expand a role to view its hierarchy.

4. In the Legend, click the **Tabular View** icon for the **User** icon. The table lists all users who have the role. You can export this information to Microsoft Excel.


Reviewing Role Hierarchies: Explained

On the Security Console you can review the role hierarchy of a job role, an abstract role, a duty role, or an HCM data role. You must have the IT Security Manager job role to perform this task.

 **Note:** Although you can review HCM data roles on the Security Console, you must manage them on the Manage HCM Data Role and Security Profiles page. Don't attempt to edit them on the Security Console.

Follow these steps:

1. Select **Navigator - Tools - Security Console**.
2. On the Security Console, ensure that **Expand Toward** is set to **Privileges**.
3. Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.
4. If the table doesn't appear by default, click the **View as Table** icon. The table lists every role inherited either directly or indirectly by the selected role. Set **Show to Privileges** to switch from roles to privileges.

 **Tip:** Enter text in the field above a column and press **Enter** to show only those roles or privileges that contain the specified text.

Click **Export to Excel** to export the current table data to Microsoft Excel.

Comparing Roles: Procedure

You can compare two roles to identify differences and similarities. The roles can be job roles, abstract roles, HCM data roles, duty roles, or aggregate privileges. You can compare roles of the same or different types. For example, you can compare a job role with a duty role or a custom job role with its predefined equivalent. This topic describes how to compare two roles.

Comparing Two Roles

Follow these steps:

1. On the Roles tab of the Security Console, click **Compare Roles**. The Compare Roles page opens.
2. In the **First Role** field, search for and select the first of the two roles to compare.
3. In the **Second Role** field, search for and select the second role.
4. Set **Show** to one of these values to identify the security artifacts to display in the comparison results:

Value	Description
All	All selected artifacts for both roles.
Only in first role	Selected artifacts that appear in the first role but not in the second role
Only in second role	Selected artifacts that appear in the second role but not in the first role
In both roles	Only those selected artifacts that appear in both roles

5. Set **Filter Criteria** to one of these values to identify the security artifacts to compare in each of the roles:
 - **Function security policies**
 - **Data security policies**
 - **Inherited roles**

For example, if you set **Filter Criteria** to **Inherited roles** and **Show** to **In both roles**, then you see the roles that both roles inherit. The comparison excludes any role that only one of the roles inherits.

6. Click **Compare**. The comparison is refreshed automatically if you change the **Show** or **Filter Criteria** values.
7. Click **Done** to close the Compare Roles page.

Alternative ways of comparing roles on the Roles tab exist. You can:

- In the search results, select **Compare Roles** from the Actions menu for a role in the search results
- In the graphical view of a role, select the role, right-click and select **Compare Roles**.

In both cases, the selected role becomes the first role in the role comparison.

Reviewing Role Information on the Analytics Tab: Explained

All roles belong to a category. In most cases, the category identifies both the owning product family and the role type. For example, HCM - Job Roles, HCM - Duty Roles, and Common - Abstract Roles are role categories. This topic describes how to review statistics relating to role categories and details of individual roles on the Analytics tab of the Security Console.

On the Analytics tab, you can see these numbers for each role category:

- Roles in the category
- Role memberships (roles that are inherited by roles in this category)

- Function security policies granted to all roles in the category
- Data security policies granted to all roles in the category

This information appears in a table. The number of roles in each category also appears in a pie chart.

Reviewing Roles on the Analytics Tab

To review role details on the Analytics tab, follow these steps:

1. Select a role category to populate the Roles in Category section of the Analytics tab.
2. In the Roles in Category section, you see a list of all roles in the selected category. You can filter the list by entering a value in any of the fields above the column headings and pressing **Enter**.
3. For a selected role, click the role name to open the Role Details page.
4. On the Role Details page, review the role's:
 - Function security policies
 - Data security policies
 - Role hierarchy
 - User memberships (users who have the role)

Click **Export** to save this role information to a .csv file.

16 Customizing Security


Copying HCM Roles: Points to Consider

Copying predefined roles and editing the copies is the recommended approach to creating custom roles. This topic describes what to consider when you're copying a role.

Reviewing the Role Hierarchy

When you copy a predefined job, abstract, or duty role, you're recommended first to review the role hierarchy. This review is to identify the inherited roles that you want to refer to, copy, or delete in your custom role. For example, the Payroll Manager job role inherits the Payroll Administrator job role, among others. When copying the Payroll Manager role, you must decide whether to copy the Payroll Administrator role, refer to it, or remove it from your copy. You can review the role hierarchy on the Roles tab of the Security Console in either graphical or tabular format. You can also:

- Export the role hierarchy to a spreadsheet from the Roles tab.
- Review the role hierarchy and export it to a spreadsheet from the Analytics tab.
- Run the User and Role Access Audit Report.


 **Tip:** Aggregate privileges are never copied. When you copy a job or abstract role, its inherited aggregate privileges are referred to from your copy.

Reviewing Privileges

Job and abstract roles inherit function security privileges and data security policies from the roles that they inherit. Function security privileges and data security policies may also be granted directly to a job or abstract role. You can review these directly granted privileges on the Roles tab of the Security Console, as follows:

- In the graphical view of a role, its inherited roles and function security privileges are visible at the same time.
- In the tabular view, you set the **Show** value to switch between roles and function security privileges. You can export either view to a spreadsheet.

Once your custom role exists, edit it to add or remove directly granted function security privileges.


 **Note:** Data security policies are visible only when you edit your custom role. You're recommended to leave data security policies unchanged.

Transaction Analysis Duty Roles

Some roles, such as the Human Resource Analyst job role, inherit Transaction Analysis Duty roles, which are used in Oracle Transactional Business Intelligence report permissions. If you copy the Human Resource Analyst job role, or any other role that inherits Transaction Analysis Duty roles, then don't copy the Transaction Analysis Duty roles. If you copy the roles, then you must update the permissions for the relevant reports to secure them using your copies of the roles. Instead, add the predefined Transaction Analysis Duty roles to your copy of the relevant job role, such as Human Resource Analyst.

Naming Copied Roles

By default, a copied role has the same name as its source role with the suffix **Custom**. The role codes of copied roles have the suffix **_CUSTOM**. Copied roles lose the prefix **ORA_** automatically from their role codes. You can define a local naming convention for custom roles, with a prefix, suffix, or both, on the Administration tab of the Security Console.

 **Note:** Copied roles take their naming pattern from the default values specified on the Administration tab of the Security Console. You can override this pattern on the Copy Role: Basic Information page for the role that you're copying. However, the names of roles inherited by the copied role are unaffected. For example, if you perform a deep copy of the Employee role, then inherited duty roles take their naming pattern from the default values.

Duplicate Roles

If any role in the hierarchy already exists when you copy a role, then no copy of that role is made. For example, if you make a second copy of the Employee role, then copies of the inherited duty roles may already exist. In this case, membership is added to the existing **copies** of the roles. To create unique copies of inherited roles, you must enter unique values on the Administration tab of the Security Console before performing a deep copy.

To retain membership of the predefined job or abstract role hierarchy, perform a shallow copy of the predefined role.

Related Topics

- [Setting Role Preferences: Explained](#)
- [User and Role Access Audit Report](#)

Security Console Role-Copy Options: Explained

When you copy a role on the Security Console, you select one of the following options:

- Copy top role
- Copy top role and inherited roles

This topic explains the effect of each of these options on the copied role.

Copy Top Role

If you select the **Copy top role** option, then memberships are created for the copy in the roles of which the original is a member. Subsequent changes to those roles appear in your copy of the role. Therefore, you can


- Add roles directly to the copied role without affecting the source role.
- Remove any role that's inherited directly by the copied role without affecting the source role.

However, if you:

- Remove any role that's inherited indirectly by the copied role, then the removal affects any role that inherits the removed role's parent role, including the source role
- Edit any inherited role, then the changes affect any role that inherits the edited role

These types of changes aren't limited to the copied role. This option is referred to as a shallow copy.

To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the **Copy top role and inherited roles** option. Alternatively, copy individual inherited roles separately, edit the copies, and use them to replace the existing versions.

 **Tip:** The Copy Role: Summary and Impact Report page provides a useful summary of your changes. Review this information to ensure that you haven't accidentally made a change that affects other roles.

Copy Top Role and Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. If you're copying a job or abstract role, then:

- Inherited aggregate privileges are never copied. Instead, membership is added to each aggregate privilege for the copied role.
- Inherited duty roles are copied if a copy with the same name doesn't already exist. Otherwise, membership is added to the existing **copies** of the duty roles for the copied application role.

When inherited duty roles are copied, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copied roles. This option is referred to as a deep copy.

Copying Upgraded Abstract Roles: Explained

This topic describes how to copy abstract roles with assigned security profiles that were upgraded from Oracle Human Capital Management Cloud Release 11. This information doesn't apply if you didn't upgrade abstract roles from Release 11.

Copying Abstract Roles

The Simplified Reference Role Model was introduced in Release 10. In Releases 10 and 11, each predefined job role and abstract role was represented as an enterprise role. The enterprise role inherited an application role. When you assigned security profiles to an abstract role before Release 12, some additional roles were generated automatically. These additional roles had the name of the abstract role with the suffix (HCM), (CRM), or (FSCM). Data security policies were generated against these roles, which were inherited directly by the abstract role's enterprise role. The presence of these roles means that the enterprise role was modified. This modification prevented the enterprise and application roles from being merged when the abstract roles were upgraded from Release 11.

As the enterprise and application roles for such abstract roles remain separate after the upgrade from Release 11, you must take care when copying them. If you perform a shallow copy of an upgraded abstract role, then you keep membership of:

- The inherited (HCM), (CRM), and (FSCM) roles.
- The application role from the original role. If the application role is predefined, then you can't edit it. Otherwise, any changes you make to the application role are also inherited by the role on which the copy was based.

Therefore, always perform a deep copy of any abstract role to which security profiles were assigned before the upgrade from Release 11. Once the copy exists, you must edit it to remove the inherited (HCM), (CRM), and (FSCM) roles. Otherwise, your custom role has the data security policies from the source role in addition to any that you create specifically for the custom role. The copied role can't function as required unless you remove these roles.


Copying Job or Abstract Roles: Procedure

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch, especially if your changes are minor. This topic explains how to copy a role to create a custom role. You must have the IT Security Manager job role to perform this task.


Copying a Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

 **Tip:** Click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

 **Tip:** The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Editing Custom Job or Abstract Roles: Procedure

You can create a custom role by copying a predefined job role or abstract role and editing the copy. This topic describes how to edit a custom role on the Security Console. You must have the IT Security Manager job role to perform this task.

Editing the Role

Follow these steps:


1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.

Managing Functional Security Privileges

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear. Select a privilege to view details of the code resources that it secures in the Details section of the page.


To remove a privilege from the role, select the privilege and click the **Delete** icon. To add a privilege to the role:

1. Click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.
7. Click **Next**.

 **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

Managing Data Security Policies

Make no changes on the Copy Role: Data Security Policies page.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Adding and Removing Inherited Roles

The Edit Role: Role Hierarchy page shows the copied role and its inherited aggregate privileges and duty roles. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the **Delete** icon.
3. Click **OK** to close the confirmation message.

To add a role:


1. Click the **Add Role** icon.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

The Edit Role: Role Hierarchy page shows the updated role hierarchy.

7. Click **Next**.

Provisioning the Role to Users

To provision the role to users, you must create a role mapping in the usual way. Don't provision the role to users here.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of user role membership** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Reviewing the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

The role is available immediately.

Creating Job or Abstract Roles from Scratch: Procedure

If the predefined roles aren't suitable or you need a role with few privileges, then you can create a role from scratch. This topic explains how to create a job role or abstract role. To perform this task, you must have the IT Security Manager job role.

Entering Basic Information

Follow these steps:

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role's display name in the **Role Name** field. For example, enter Sales Department Administration Job Role.
3. Complete the **Role Code** field. For example, enter SALES_DEPT_ADMIN_JOB.
Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**.
4. In the **Role Category** field, select either **HCM - Abstract Roles** or **HCM - Job Roles**, as appropriate.
5. Click **Next**.


Adding Functional Security Policies

When you create a role from scratch, you're most likely to add one or more aggregate privileges or duty roles to your role. You're less likely to grant function security privileges directly to the role.

If you aren't granting function security privileges, then click **Next**. Otherwise, to grant function security privileges to the role:


1. On the Create Role: Functional Security Policies page, click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from a selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.

6. Close the **Add Function Security Policy** dialog box.
7. Click **Next**.

 **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

Creating Data Security Policies

Make no entries on the Create Role: Data Security Policies page.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Building the Role Hierarchy


The Create Role: Role Hierarchy page shows the hierarchy of your custom role in tabular format by default. You can add one or more aggregate privileges, job roles, abstract roles, and duty roles to the role. Typically, when creating a job or abstract role you add aggregate privileges. Roles are always added directly to the role that you're creating.

To add a role:

1. Click the **Add Role** icon.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. When you finish adding roles, close the **Add Role Membership** dialog box.
7. Click **Next**.

Provisioning the Role

To provision the role to users, you must create a role mapping in the usual way once the role exists. Don't provision the role to users here.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of user role membership** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Reviewing the Role

On the Create Role: Summary and Impact Report page, review the summary of the changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

Your custom role is available immediately.


Copying and Editing Duty Roles: Procedure

You can copy a duty role and edit the copy to create a custom duty role. Copying duty roles is the recommended way of creating custom duty roles. This topic explains how to copy a duty role and edit the copy. You must have the IT Security Manager job role to perform these tasks.


Copying a Duty Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the duty role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

 **Tip:** Click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

 **Tip:** The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Editing the Copied Duty Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.


Managing Functional Security Policies

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear. Select a privilege to view details of the code resources that it secures.

To remove a privilege from the role, select the privilege and click the **Delete** icon. To add a privilege to the role:


1. Click **Add Function Security Policy**.

2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to grant all function security privileges from the selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Functional Security Policies** dialog box.
7. Click **Next**.

 **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

Managing Data Security Policies

Make no changes on the Edit Role: Data Security Policies page.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Adding and Removing Inherited Roles

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles and aggregate privileges that it inherits. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the **Delete** icon.
3. Click **OK** to close the information message.

To add a role:

1. Click **Add Role**.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

The Edit Role: Role Hierarchy page shows the updated role hierarchy.

7. Click **Next**.

Reviewing the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

The role is available immediately.

17 Regenerating Roles

Regenerating Roles: Explained

You must regenerate an HCM data role if you change its role hierarchy. For example, if you remove an aggregate privilege from a custom job role, then you must regenerate any data role that inherits the job role. You must also regenerate any abstract role to which security profiles are assigned if you change its role hierarchy. Regenerating a role updates its data security policies to reflect the latest role hierarchy. This topic introduces the ways in which you can regenerate data and abstract roles.

Regenerating Multiple Roles

To regenerate multiple roles at once, you use the Process Grants Regeneration process. Before you can use this process, you must add the **Resubmit All Roles** button to the Manage Data Roles and Security Profiles page. Adding this button is a once-only task.


Regenerating a Role

To regenerate a single data or abstract role, you can use the Process Grants Regeneration process. Alternatively, you can edit the role on the Manage Data Roles and Security Profiles page.

Follow these steps:

1. Search for the data or abstract role.
2. Select the role in the Search Results and click **Edit**.
3. On the Edit Data Role: Select Role page, click **Next**.
4. On the Edit Data Role: Security Criteria page, click **Review**.
5. 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.

 **Note:** You must regenerate updated, predefined roles after each release upgrade of Oracle HCM Cloud. For example, if the predefined Payroll Manager role is updated in an upgrade, then you must regenerate any data role that inherits that job role.

Enabling the Grants Regeneration Process: Procedure

You can regenerate HCM data roles and abstract roles individually by editing them on the Manage Data Roles and Security Profiles page. Alternatively, to regenerate one or more roles, you can run the Process Grants Regeneration process. This topic describes how to enable this process by adding the **Resubmit All Roles** button to the Manage Data Roles and Security Profiles page. You perform this task once only.


Adding the Resubmit All Roles Button

Follow these steps:

1. Sign in with the following roles or privileges:
 - IT Security Manager
 - Application Implementation Consultant or Human Capital Management Application Administrator
2. Create and activate a sandbox.
3. Select **Navigator - Workforce Structures**.
4. In the Tasks panel tab of the Workforce Structures work area, select Manage Data Roles and Security Profiles.

 **Note:** Don't select this task in the Setup and Maintenance work area. Select it in the Workforce Structures work area.

5. In the Settings and Actions menu in the global header, select **Customize Pages...** to open the Page Composer. Follow these steps to add the **Resubmit All Roles** button to the Manage Data Roles and Security Profiles page.
 - a. In the dialog box that opens, select the **Site** layer and click **OK**.
 - b. From the View menu in the Page Composer, select **Source**. This option opens a source-code area at the bottom of the page.
 - c. Expand the source-code area to show more of the content.
 - d. Move the cursor to the Manage Data Roles and Security Profiles page header and left-click. In the warning about editing a shared component, click **Edit**.

 **Note:** You aren't editing the page header, but this approach provides a quick way to find the **Resubmit All Roles** button in the source code.

- e. The toolbar component that contains the **Resubmit All Roles** button opens in the source-code area.
 - f. In the source-code area, right-click the **commandToolbarButton: Resubmit All Roles** entry and click **Show Component**. The **Resubmit All Roles** button now appears on the Manage Data Roles and Security Profiles page.
6. Close the Page Composer.
 7. Select the sandbox, click **More**, and publish your changes.

The **Resubmit All Roles** button is now available to all users of the Manage Data Roles and Security Profiles page to regenerate roles.


Regenerating Multiple Data and Abstract Roles: Procedure

You must regenerate an HCM data role if changes are made to the data security policies of its inherited job role. For example, if an aggregate privilege is removed from the job role, then you must regenerate any data role that inherits the job role. You must also regenerate any abstract role that has directly assigned security profiles if changes are made to the role's data security policies. You can regenerate data and abstract roles individually by editing them on the Manage Data Roles and Security Profiles page. Alternatively, to regenerate one or more roles, you can run the Process Grants Regeneration process. This topic describes how to run this process.

Running Process Grants Regeneration

Follow these steps.

1. Sign in with the IT Security Manager role or privileges and select **Navigator - Workforce Structures**.
2. In the Tasks panel tab of the Workforce Structures work area, select the Manage Data Roles and Security Profiles task.
3. On the Manage Data Roles and Security Profiles page, click **Resubmit All Roles**.

 **Note:** The **Resubmit All Roles** button doesn't appear by default. You must configure the page to include this button. Configuring the page is a once-only task.

The Process Flow page opens.

4. On the Process Flow page, click **Schedule**.
5. On the Schedule page, click the **Process Grants Regeneration** name. The Schedule: Process Grants Regeneration page opens.
6. On the Schedule: Process Grants Regeneration page:
 - a. In the **Process Flow** field, enter a name for this run of the process. You can enter any text that helps you to identify this run.
 - b. In the **Mode** field, select a value. This table describes the values.

Mode Value	Description
Named Job Role	Regenerates any data role that inherits the specified job role directly. Data roles that inherit the job role indirectly aren't regenerated.
Named Data Role	Regenerates the specified data role only.
Named Abstract Role	Regenerates the specified abstract role only.
Process All Roles	Regenerates all roles to which security profiles are assigned. In this mode, secured access for all roles is recalculated and the secured access of all users is refreshed. The time taken to complete this process depends on the number of roles to be regenerated.

- c. If you're regenerating a named role, then select a **Role** value.
- d. Select a **Run** value.
- e. Click **Submit**.

On the Process Flow page, the processing information refreshes automatically while the process is running. You can open other pages and return to this page to review progress. When the process completes, click the process run name to see the process results. The Process Flow page shows the name that you specified for this run. The Process Results section of the page lists all roles that were processed and indicates whether the regeneration succeeded.

7. Click **Done** to close the page.

18 Security and Reporting

Oracle Fusion Transactional Business Intelligence Security: Explained

Oracle Fusion Transactional Business Intelligence is a real-time, self-service reporting solution. All application users with appropriate roles can use Transactional Business Intelligence to create analyses that support decision-making. In addition, business users can perform current-state analysis of their business applications using a variety of tools. These include Oracle Business Intelligence Enterprise Edition as the standard query and reporting tool, Oracle Business Intelligence Answers, and Oracle Business Intelligence Dashboard end-user tools. This topic summarizes how access is secured to Transactional Business Intelligence subject areas, Business Intelligence Catalog folders, and Business Intelligence 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**).

This table identifies the subject areas that predefined HCM job roles can access.

HCM Job Role	Subject Areas
Benefits Manager	All Benefits
Compensation Manager	All Compensation
Compensation Analyst	All Compensation
Human Resource Analyst	Goals, Workforce Management, Workforce Performance, Workforce Profiles, and Talent Review
Line Manager	All Workforce Management
Payroll Manager	All Payroll

Analyses fail if the user can't access all subject areas in a report.

Business Intelligence Catalog Folders

Business Intelligence 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 Business Intelligence Catalog and the Workforce Management subject areas.

This table identifies the folders that predefined HCM job roles can access.

HCM Job Role	Business Intelligence Catalog Folders
Benefits Manager	Transactional Business Intelligence Benefits
Compensation Manager	Transactional Business Intelligence Compensation
Compensation Analyst	Transactional Business Intelligence Compensation
Human Resource Analyst	Business Intelligence Publisher Goals, Performance, and Profiles Transactional Business Intelligence Career and Workforce Management
Line Manager	Business Intelligence Publisher Compensation and Workforce Management Transactional Business Intelligence Workforce Management and many Business Intelligence Answers folders
Payroll Manager	Transactional Business Intelligence and Business Intelligence Answers Payroll folders

Business Intelligence Reports

Analyses are secured based on the folders in which they're stored. If you haven't secured Business Intelligence reports using the report privileges, then they're secured at the folder level by default. You can set permissions against folders and reports 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

How Reporting Data Is Secured: Explained

The data that's returned in Oracle Transactional Business Intelligence reports is secured in a similar way to the data that's returned in application pages. Data access is granted by roles that are linked to security profiles. This topic describes the part played by Transaction Analysis Duty Roles in securing access to data in Transactional Business Intelligence reports. It also describes how to enable this access in custom job roles.

Transaction Analysis Duty Roles

Each of the Transaction Analysis Duty roles providing access to subject areas and Business Intelligence Catalog folders is granted one or more data security policies. These policies enable access to the data.


Custom Job Roles

If you create a custom job role with access to Transactional Business Intelligence reports, then you must give the role the correct duty roles. Your custom role must have 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 must access the Workforce Transaction Analysis subject areas, then it must inherit the following duty roles:

Duty Role	Version
Workforce Transaction Analysis Duty	OBI
Workforce Transaction Analysis	HCM

The Workforce Transaction Analysis Duty role is granted relevant data security policies and inherits BI Consumer Role.

 **Note:** You're recommended not to copy the OBI Transaction Analysis Duty roles. Instead, add the predefined OBI Transaction Analysis Duty roles to your custom role. If you copy the roles, then you must update the permissions for relevant reports to secure them using your copies of the roles.

Business Intelligence Roles: Explained

Oracle Business Intelligence roles apply to both Oracle Business Intelligence Publisher and Oracle Fusion Transactional Business Intelligence. They grant access to Business Intelligence functionality, such as the ability to run or author reports. These roles are in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and HCM data. This topic describes the Business Intelligence roles.

This table lists the Business Intelligence roles.

Business Intelligence Role	Description
BI Consumer Role	Runs Business Intelligence reports.
BI Author Role	Creates and edits reports.
BI Administrator Role	Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.
BI Publisher Data Model Developer Role	Creates and edits Business Intelligence Publisher data models.

BI Consumer Role

The predefined Transactional Business Intelligence Transaction Analysis Duty roles inherit 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

BI Author Role inherits BI Consumer Role. Users with BI Author Role can create, edit, and run Transactional Business Intelligence reports.

BI Administrator Role

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role. 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 Business Intelligence Publisher data models.

Viewing Reporting Roles and Permissions: Procedure

Viewing reporting roles and permissions can help you to understand how Oracle Transactional Business Intelligence security works.

This topic explains how to view:

- The reporting roles that a job role inherits
- The permissions for sample Oracle Transactional Business Intelligence reports in the Business Intelligence Catalog

Viewing Inherited Reporting Roles on the Security Console

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

1. Select **Navigators - Tools - Security Console**.
2. On the Security Console, search for and select a job role. For example, search for and select the Human Resource Analyst job role.

Depending on the enterprise setting, either a graphical or a tabular representation of the role appears. Switch to the tabular view if it doesn't appear by default.
3. Human Resource Analyst inherits many Transaction Analysis duty roles, such as Documents of Record Transaction Analysis and Absence Management Transaction Analysis. These roles (without the word Duty in their names) are **HCM** roles. Their role codes start with the characters **ORA_**. Find these roles in the table.
4. Notice also the many Transaction Analysis Duty roles (with the word Duty in their names) that appear here. For example, Human Resource Analyst inherits the Documents of Record Transaction Analysis Duty and Absence

Management Transaction Analysis Duty roles. These roles are **OBI** roles. Their role codes start with the characters **FBI_**. Find these roles in the table.

5. Notice that the Absence Management Transaction Analysis Duty role inherits BI Consumer Role. Most of the **OBI** duty roles inherit BI Consumer Role.
6. The Human Resource Analyst role inherits BI Author Role directly. Find BI Author Role. Notice that BI Author Role also inherits BI Consumer Role.

 **Tip:** You can export the role hierarchy to a spreadsheet for offline review.

Viewing Permissions in the Business Intelligence 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 the **Browse Catalog** icon. 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 **Transactional Analysis Samples** folder.
A list of reports appears on the BI Catalog page.
5. Under **Costing Reports**, click **More - Permissions**.
The Permissions dialog box opens. Scroll if necessary to see the complete list of permissions, which includes the role BI Administrator Role.
6. Click the Oracle Applications tab to return to the home page.

Business Intelligence Publisher Secured List Views: Explained

Oracle Business Intelligence Publisher is a set of tools for creating formatted reports based on data models. You can access Business Intelligence Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking **New - Report**. This topic describes how you can use secured list views to secure access to data in Business Intelligence 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, Business Intelligence Publisher separates the data model, layout, and translation. Therefore, 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

Business Intelligence Publisher Data Security and Secured List Views

When you create a Business Intelligence Publisher data model with physical SQL, 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, 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 tables show, 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

These duty roles have the privileges in the following table:

- Absence Management Transaction Analysis
- Payroll Transaction Analysis
- Vacancy Transaction Analysis
- Workforce Transaction Analysis

Table	Secured List View	Data Security Privilege
HR_ALL_ORGANIZATION_UNITS_F	PER_DEPARTMENT_SECURED_LIST_V	Report Department Data
HR_ALL_POSITIONS_F	PER_POSITION_SECURED_LIST_V	Report Position Data
PER_JOBS_F	PER_JOB_SECURED_LIST_V	Report HR Job Data
PER_LOCATIONS	PER_LOCATION_SECURED_LIST_V	Report Location Data
PER_GRADES_F	PER_GRADE_SECURED_LIST_V	Report Assignment Grade Data

 **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.

These duty roles have the privileges in the following table:

- Documents of Record Transaction Analysis
- Payroll Transaction Analysis
- Workforce Transaction Analysis

Table	Secured List View	Data Security Privilege
PER_ALL_PEOPLE_F	PER_PERSON_SECURED_LIST_V	Report Person Data
PER_PERSONS	PER_PUB_PERS_SECURED_LIST_V	Report Person Deferred Data

The Payroll Transaction Analysis duty role has the privileges in the following table:

Table	Secured List View	Data Security Privilege
HR_ALL_ORGANIZATION_UNITS_F	PER_LEGAL_EMP_SECURED_LIST_V	Report Legal Employer Data
PER_LEGISLATIVE_DATA_GROUPS	PER_LDG_SECURED_LIST_V	Report Legislative Data Group Data
PAY_ALL_PAYROLLS_F	PAY_PAYROLL_SECURED_LIST_V	Report Payroll Definition Data

The Compensation Transaction Analysis duty role has the privileges in the following table:

Table	Secured List View	Data Security Privilege
CMP_SALARY	CMP_SALARY_SECURED_LIST_V	Report Salary Data

The Human Resource Analyst job role has the privilege in the following table:

Table	Secured List View	Data Security Privilege
PER_ALL_ASSIGNMENTS_M	PER_ASSIGNMENT_SECURED_LIST_V	Report Assignment Data

You can find details of the secured list views in the Tables and Views for Oracle HCM Cloud guide on the Oracle Help Center.

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 Oracle Business Intelligence 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 tables that contain PII data and the data security privileges that are used to report on them.

Tables Containing PII Information

This table lists the PII tables and the privileges that are used to report on data in these tables.

Table	Data Security Privilege
PER_ADDRESSES_F	Report Person Address
PER_CONTACT_RELSHIPS_F	Report Person Contact
PER_DRIVERS_LICENSES	Report Driver License
PER_EMAIL_ADDRESSES	Report Person Email
PER_NATIONAL_IDENTIFIERS	Report Person National Identifier

Table	Data Security Privilege
PER_PASSPORTS	Report Person Passport
PER_PERSON_DLVRY_METHODS	Report Person Communication Method
PER_PHONES	Report Person Phone
PER_VISAS_PERMITS_F	Report Person Visa

 **Note:** Work e-mail and phone aren't protected.

All of these privileges are accessible using the Workforce Confidential Reporting duty role, which the Human Resource Analyst job role inherits.

Dimension Security: Explained

A dimension is a collection of business attributes or a hierarchy structure that you use to group or aggregate numeric measures. All Oracle Transactional Business Intelligence dimensions are unsecured, except for the Assignment Manager dimension. Therefore, when you select a single dimension, such as the worker or department dimension, you can see all worker and department data unfiltered. Oracle Transactional Business Intelligence data security isn't applied until you select more than one dimension or one dimension plus one or more metrics.

For example, if you select Department Name from the Workforce Management - Worker Assignment Real Time subject area, then you can view all departments. When you add Assignment Count to the report, data security is applied and you can view workers only in the departments that you can access.

Assignment Manager

Assignment Manager is a hierarchical structure representing the reporting relationship between workers and managers. This dimension is the only secured HCM dimension in Oracle Transactional Business Intelligence. The Assignment Manager hierarchy is restricted to line managers. If the signed-in user doesn't have direct reports, then he or she sees no data when you include Assignment Manager in the report.

Reserve the use of Assignment Manager for line managers only. Some other job roles, such as human resource analyst, may need access to manager information. In these cases, use the Manager Name in the Worker dimension instead of the Assignment Manager hierarchy.

FAQs for Security and Reporting

How can I give line managers access to compensation subject areas?

The predefined Line Manager role has no access to compensation subject areas. To provide this access, create a custom Line Manager job role. Add both the Compensation Transaction Analysis Duty and Compensation Transaction Analysis roles to the custom role.

How can I give line managers access to talent management subject areas?

The predefined Line Manager role has no access to talent management subject areas. To provide this access, create a custom Line Manager role. Add relevant transaction analysis duty roles to the custom role. For example, you may want to provide access to Workforce Goals subject areas. In this case, add both the Goal Management Transaction Analysis Duty and Goal Management Transaction Analysis roles to your custom role.

19 Certificate Management

Managing Certificates: Explained

Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications. Use the Certificates page in the Security Console functional area to work with certificates in either of two formats, PGP and X.509.

For each format, a certificate consists of a public key and a private key. The Certificates page displays one record for each certificate. Each record reports these values:

- **Type:** For a PGP certificate, "Public Key" is the only type. For an X.509 certificate, the type is either "Self-Signed Certificate" or "Trusted Certificate" (one signed by a certificate authority).
- **Private Key:** A check mark indicates that the certificate's private key is present. For either certificate format, the private key is present for your own certificates (those you generate in the Security Console). The private key is absent when a certificate belongs to an external source and you import it through the Security Console.
- **Status:** For a PGP certificate, the only value is "Not Applicable." (A PGP certificate has no status.) For an X.509 certificate, the status is derived from the certificate.

To the right in the row for each certificate, click a button to display a menu of actions appropriate for the certificate. Or, to view details for a certificate, select its name ("alias"). Actions include:

- Generate PGP or X.509 certificates.
- Generate signing requests to transform X.509 certificates from self-signed to trusted.
- Export or import PGP or X.509 certificates.
- Delete certificates.

Generating Certificates: Explained

For a PGP or X.509 certificate, one operation creates both the public and private keys. From the Certificates page, select the Generate option. In a Generate page, select the certificate format, then enter values appropriate for the format.

For a PGP certificate, these values include:

- An alias (name) and passphrase to identify the certificate uniquely.
- The algorithm by which keys are generated, DSA or RSA.
- A key length.

For an X.509 certificate, these values include:

- An alias (name) and private key password to identify the certificate uniquely.
- A common name, which is an element of the "distinguished name" for the certificate. The common name identifies the entity for which the certificate is being created, in its communications with other web entities. It must match the name of the entity presenting the certificate. The maximum length is 64 characters.

- Optionally, other identifying values: Organization, Organization Unit, Locality, State/Province, and Country. These are also elements of the distinguished name for the certificate, although the Security Console does not perform any validation on these values.
- An algorithm by which keys are generated, MD5 or SHA1.
- A key length.
- A validity period, in days. This period is preset to a value established on the General Administration page. You can enter a new value to override the preset value.

Generating a Signing Request: Procedure

You can generate a request for a certificate authority (CA) to sign a self-signed X.509 certificate, to make it a trusted certificate. (This process does not apply to PGP certificates.)

1. Select **Generate Certificate Signing Request**. This option is available in either of two menus:
 - One menu opens in the Certificates page, from the row for a self-signed X.509 certificate.
 - The other menu is the Actions menu in the details page for that certificate.
2. Provide the private key password for the certificate, then select a file location.
3. Save the request file. Its default name is [alias]_CSR.csr.

You are expected to follow a process established by your organization to forward the file to a CA. You would import the trusted certificate returned in response.

Importing and Exporting X.509 Certificates: Procedure

For an X.509 certificate, you import or export a complete certificate in a single operation.

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Certificate.
3. Select a location for the export file. By default, this file is called [alias].cer.

To import, use either of two procedures. Select the one appropriate for what you want to do:

- The first procedure replaces a self-signed certificate with a trusted version (one signed by a CA) of the same certificate. (A prerequisite is that you have received a response to a signing request.)
 - a. In the Certificates page, locate the row for the self-signed certificate, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
 - b. Enter the private key password for the certificate.
 - c. Browse for and select the file returned by a CA in response to a signing request, and click the Import button. In the Certificates page, the type value for the certificate changes from self-signed to trusted.
- The second procedure imports a new X.509 certificate. You can import a .cer file, or you can import a keystore that contains one or more certificates.
 - a. In the Certificates page, click the Import button. An Import page opens.

- b. Select X.509, then choose whether you are importing a certificate or a keystore.
- c. Enter identifying values, which depend on what you have chosen to import. In either case, enter an alias (which, if you are importing a .cer file, need not match its alias). For a keystore, you must also provide a keystore password and a private key password.
- d. Browse for and select the import file.
- e. Select Import and Close.

Importing and Exporting PGP Certificates: Procedure

For a PGP certificate, you export the public and private keys for a certificate in separate operations. You can import only public keys. (The assumption is that you will import keys from external sources, who will not provide their private keys to you.)

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Public Key or Private Key.
3. If you selected Private Key, provide its passphrase. (The public key does not require one.)
4. Select a location for the export file. By default, this file is called [alias]_pub.asc or [alias]_priv.asc.

To import a new PGP public key:

1. On the Certificates page, select the Import button.
2. In the Import page, select PGP and specify an alias (which need not match the alias of the file you are importing).
3. Browse for the public-key file, then select Import and Close.

The Certificates page displays a record for the imported certificate, with the Private Key cell unchecked.

Use a distinct import procedure if you need to replace the public key for a certificate you have already imported, and do not want to change the name of the certificate:

1. In the Certificates page, locate the row for the certificate whose public key you have imported, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
2. Browse for the public-key file, then select Import.

Deleting Certificates: Procedure

You can delete both PGP and X.509 certificates:

1. In the Certificates page, select the menu available in the row for the certificate you want to delete. Or, in the details page for that certificate, select the Actions menu.
2. In either menu, select Delete.
3. Respond to a warning message. If the certificate's private key is present, you must enter the passphrase (for a PGP certificate) or private key password (for an X.509 certificate) as you respond to the warning. Either value would have been created as your organization generated the certificate.

20 Role Optimization

Role Optimizer: Explained

Role optimization is the process used to analyze the existing role hierarchy for redundancies or other inefficiencies. Role optimization enables you to create a role hierarchy that minimizes the number of roles necessary to authorize every job role to its currently authorized privileges. The role optimizer feature automates the analysis process and generates a report you can use to optimize your job hierarchies.

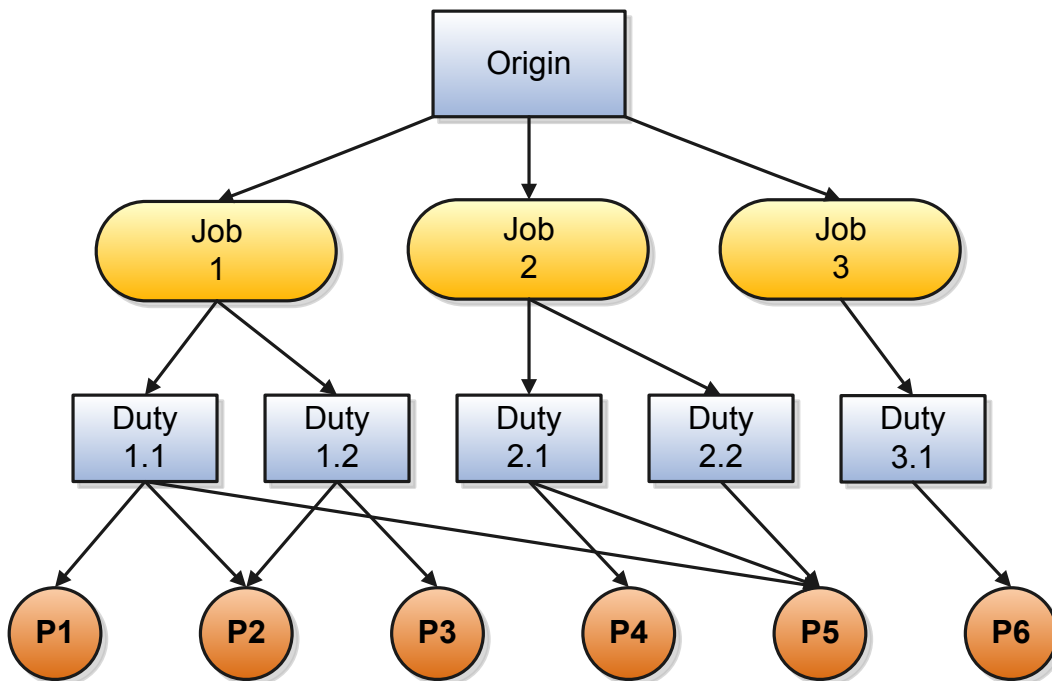
❗ Important: The use of the Role Optimization Report is not included in the cost of your service subscription or application license and incurs charges in addition to your subscription or licensing fee.

Reasons to Optimize

Changes to the predefined role hierarchies can put the privacy of your application data at risk. You can unintentionally make your data less secure if you:

- Create duty roles with small groups of privileges in an attempt to minimize:
 - Dependencies
 - The impact of making incremental changes
- Grant privileges that already exist in the role hierarchy

Roles can proliferate or have duplicate privileges over time to make your role hierarchy less efficient, as you see in the following figure.



Benefits of Optimization

By using the role optimizer, you can:

- Increase user productivity.

You save time that you can perform other tasks.

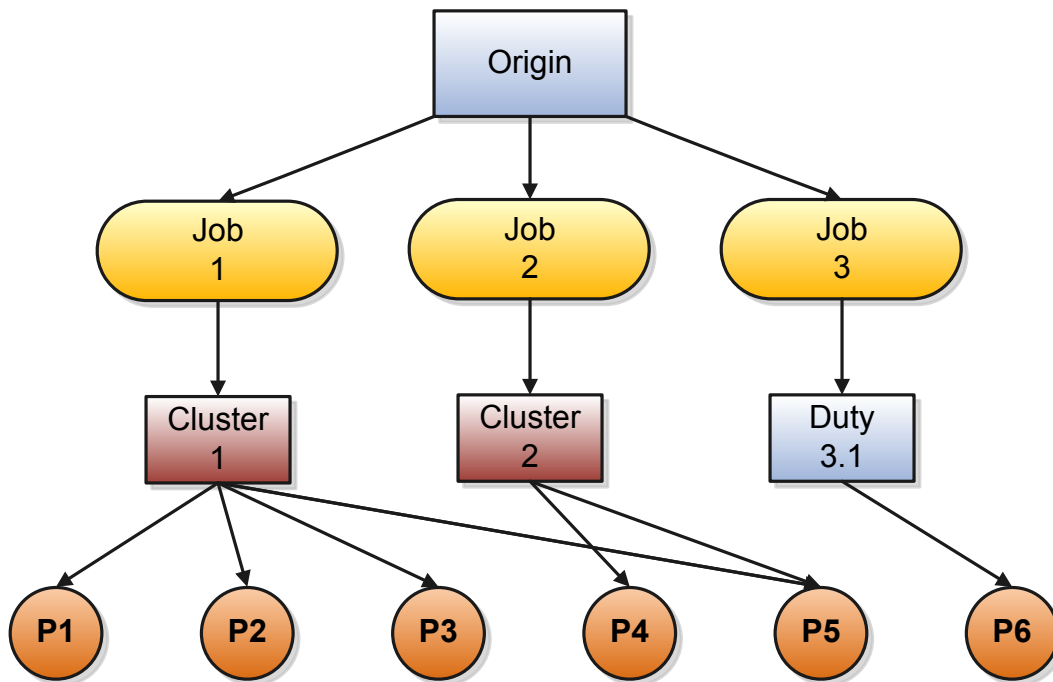
- Lower administrative costs.

You reduce the number of security objects and the amount of time you spend maintaining that you must administer them.

- Decrease access risk associated with undocumented role hierarchy changes.

You identify and can eliminate redundant and inappropriate grants of privilege.

The role optimizer can suggest more efficient role hierarchies, such as the one you see in this figure.



Role Optimizer Access

The role optimizer feature is available as a predefined report. Schedule and submit the Role Optimization Report on the Overview page of the Scheduled Processes work area. The process:

1. Analyzes your existing job role hierarchies.
2. Generates the optimized job role hierarchy and stores the data for each job role in a separate CSV file.
3. Archives and attaches the CSV files as the process output.
4. Generates a log and archives it as a ZIP file. The log file includes technical details of the analysis for troubleshooting.

❗ Important: The role optimization process makes no changes to your security structures. You use the report to map privileges to roles and update the role hierarchies.

Role Optimization Report

Use the Role Optimization Report to create the most efficient role hierarchy for your organization. Use the report results to evaluate and, if necessary, update your role hierarchy. The report results enable you to create a role hierarchy with the minimum number of roles necessary to authorize every job role to every privilege it is currently authorized to.

❗ Important: The use of the Role Optimization Report is not included in the cost of your service subscription or application license and incurs charges in addition to your subscription or licensing fee.

Users with the IT Security Manager role can run the Role Optimization Report, which is available from the security console.

You should run this report if you:

- Make changes to the predefined role hierarchy.
- Implement your own role hierarchy instead of the predefined role hierarchy.

! Important: The process makes no changes to your role hierarchies.

Note: The predefined role hierarchy in the security reference implementation is optimized as delivered.

Report Files

Monitor the process status on the Overview page. When the status value is Succeeded, two files appear in the **Log and Output** section of the report details. The following table describes the two files:

File Name	Description
ClusterAnalysis-Job-CSVs. zip	<p>Contains one CSV file for every job role. Each CSV file contains the duty roles and privileges that make up the optimized job role hierarchy. The name of a CSV file, identifies the job role hierarchy data that the file contains.</p> <p>For example, the ClustersforJob-AR_REVENUE_MANAGER_JOB_14240.csv file contains all of the role hierarchy data for the Accounts Receivables Revenue Manager job role.</p>
Diagnostics. zip	Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.

Import the raw data from the CSV file into your preferred application to read the results. Report data appears in these two sections:

- Privilege Clusters
- Cluster Details

Role Optimization Report Results

Privilege Clusters

The Privilege Clusters section lists each privilege and the name of a recommended privilege cluster. Specific cluster recommendations are described in the cluster details section.

Cluster Details

A Cluster Details section appears for each privilege cluster referenced in the Privilege Clusters section. Each detail section includes:

- Cluster name.
- Names of recommended candidate roles that map to the privilege cluster.
- Names and descriptions of the jobs and privileges associated with the cluster.

This table provides descriptions of the fields that appear the Cluster Details section:

Field Name	Description
Cluster Name	The name of the optimized cluster, usually in this format: Cluster ###
Primary, Secondary, Tertiary Candidate Role	<p>Recommended role mappings for the privileges in the cluster. Up to three recommended duty roles map to the listed privileges.</p> <p>Select a role. Then assign the privileges in the cluster to that role.</p>
Jobs in Cluster	<p>The number of job roles that inherit the privilege cluster.</p> <p>A list of job names and descriptions is also included.</p>
Privileges in Cluster	<p>The number of privileges that make up the cluster.</p> <p>A list of privilege names and descriptions is also included.</p>

21 Advanced Data Security

Advanced Data Security: Explained

Advanced Data Security offers two types of extended data protections. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest. Advanced Data Security is available for Oracle Applications Cloud by subscription to Break-Glass service.

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and system administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects.

Administrators can perform regular database maintenance activities, but cannot select from the application tables. If a DBA requires access to the application tables, she can request temporary access to the Fusion schema at which point keystroke auditing is enabled.

Transparent Data Encryption

Transparent Data Encryption (TDE) protects Fusion Applications data which is at rest on the file system from being read or used. Data in the database files (DBF) is protected because DBF files are encrypted. Data in backups and in temporary files is protected. All data from an encrypted tablespace is automatically encrypted when written to the undo tablespace, to the redo logs, and to any temporary tablespace.

Advanced security enables encryption at the tablespace level on all tablespaces which contain applications data. This includes SOA tablespaces which might contain dehydrated payloads with applications data.

Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL). Tablespace keys are stored in the header of the tablespace and in the header of each operating system (OS) file that makes up the tablespace. These keys are encrypted with the master key which is stored in the Oracle Wallet. Tablespace keys are AES128-bit encryption while the TDE master key is always an AES256-bit encryption.

Glossary

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.

action

The kind of access, such as view or edit, named in a security policy.

aggregate privilege

A predefined role that combines one function security privilege with related data security policies.

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.

business unit

A unit of an enterprise that performs one or many business functions that can be rolled up in a management hierarchy.

condition

The part of 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.

data dimension

A stripe of data accessible by a user. Sometimes referred to as data security context.

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 and 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.

delegated role

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

department

A division of a business enterprise dealing with a particular area of activity.

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 application 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.

enterprise

An organization with one or more legal entities under common control.

entitlement

Grant of access to functions and data. Oracle Fusion Middleware term for privilege.

function security

The control of access to a page or a specific use of a page. Function security controls what a user can do.

generic organization hierarchy

An organization hierarchy that includes organizations of all classifications.

grade

A component of the employment model that defines the level of compensation for a worker.

HCM

Abbreviation for Human Capital Management.

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, such as an accounts payable manager or application implementation consultant, that usually identifies and aggregates the duties or responsibilities that make up the job.

LDAP

Abbreviation for Lightweight Directory Access Protocol.

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 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.

party

A physical entity, such as a person, organization or group, that the deploying company has an interest in tracking.

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 assignment level.

position

A specific occurrence of one job that is fixed within one department. It is also often restricted to one location. For example, the position Finance Manager is an instance of the job Manager in the Finance Department.

privilege cluster

In the output of the Role Optimization Report, a group of privileges that you can map to a duty role.

public person

A person for whom basic information, such as name and phone, is available to all workers in worker directories and elsewhere.

resource

People designated as able to be assigned to work objects, for example, service agents, sales managers, or partner contacts. A sales manager and partner contact can be assigned to work on a lead or opportunity. A service agent can be assigned to a service request.

role

Controls access to application functions and data.

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.

sandbox

A testing environment that isolates untested code changes from the mainline environment so that these changes don't affect the mainline metadata or other sandboxes.

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 that includes role based access control, and policies that protect functions, and data. 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.

SQL predicate

A type of condition using SQL to constrain the data secured by a data security policy.

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 the tasks, searches, and other content you need to accomplish a business goal.

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.

worker type

A classification selected on a person's work relationship, which can be employee, contingent worker, pending worker, or nonworker.