Oracle Fusion Cloud HCM

Securing HCM

24B

Oracle Fusion Cloud HCM
Securing HCM

24B

F92765-01

Copyright © 2011, 2024, Oracle and/or its affiliates.

Author: Prashanth Rayakar

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Use help icons ? to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 An Introduction to HCM Security in the Cloud

Overview of Securing Oracle HCM Cloud

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 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.
Working with the Bridge for Microsoft Active Directory	How to install and configure the bridge for Microsoft Active Directory and synchronize user accounts
Managing Location-Based Access	How to enable location-based access, list authorized IP addresses, and make selected roles public
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

Chapter	Contents
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
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
Creating and Editing Job, Abstract, and Duty Roles	How to copy predefined roles to create roles, how to create roles from scratch, and how to edit custom roles
Regenerating Roles	How to regenerate the data security policies of data and abstract roles when the role hierarchy changes
Securing Access to Value Sets	How value sets are secured, and how APPID users gain access to secured value sets
Securing Content Sections in Person Profiles	How to secure user access to content-type data in person profiles
Securing Access to Succession Plans, Incumbents, and Candidates	How to create a super user role to enable access to all succession plans, and how to configure restricted access to lists of incumbents and candidates
Securing Access to Lists of Values in Responsive User Experience Pages	How to enable custom roles to access lists of values in responsive user experience pages
Security and Reporting	How to enable users to run Oracle Transactional Business Intelligence and Oracle Business Intelligence Publisher reports
Roles for Workflow Access	The predefined roles that enable access to workflow functionality
Auditing Oracle HCM Cloud Business Objects	How to configure audit for HCM business objects and access audit 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

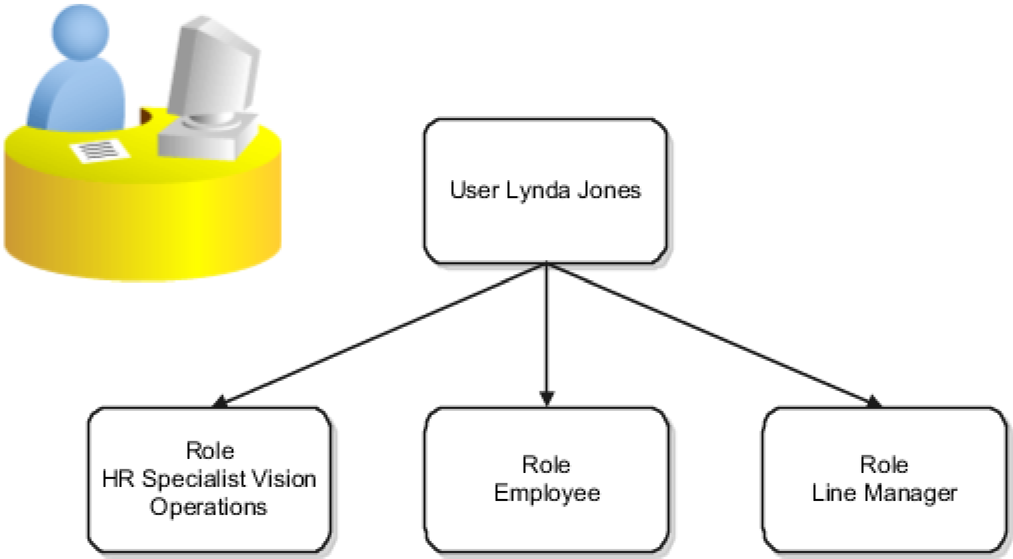
Chapter	Contents
Advanced Data Security	An introduction to these optional cloud services: • Database Vault for Oracle Fusion Human Capital Management Security Cloud Service • Transparent Data Encryption for Oracle Fusion Human Capital Management Security Cloud Service

During implementation, you perform security-related tasks from a functional area task list or implementation project. After 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

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.

This table summarizes 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

This table provides some examples of role-based access.

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

Many job and abstract roles are predefined in Oracle Human Capital Management Cloud (Oracle HCM Cloud).

The predefined HCM job roles are:

- Benefits Administrator
- Benefits Manager
- Benefits Specialist
- Cash Manager
- Compensation Administrator
- Compensation Analyst
- Compensation Manager
- Compensation Specialist
- Corporate Social Responsibility Manager

- Employee Development Manager
- Employee Wellness Manager
- Environment, Health, and Safety Manager
- Human Capital Management Application Administrator
- Human Capital Management Integration Specialist
- Human Resource Analyst
- Human Resource Help Desk Administrator
- Human Resource Help Desk Agent
- Human Resource Help Desk Manager
- Human Resource Manager
- Human Resource Specialist
- IT Auditor
- Knowledge Author HCM
- Knowledge Search HCM
- Learning Specialist
- Payroll Administrator
- Payroll Manager
- Recruiter
- Recruiting Administrator
- Time and Labor Administrator
- Time and Labor Manager

The predefined HCM abstract roles are:

- Contingent Worker
- Employee
- Executive Manager
- Hiring Manager
- Job Application Identity for Recruiting
- Line Manager
- Pending Worker

These predefined job and abstract 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 abstract roles, such as Employee and Line Manager, directly to users.

Role Types

This topic introduces the role types in Oracle Human Capital Management Cloud (Oracle HCM Cloud).

Oracle HCM Cloud defines five types of roles:

- Data roles
- Abstract roles
- Job roles
- Aggregate privileges
- Duty roles

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. The three main abstract roles predefined in Oracle HCM Cloud are:

- Employee (ORA_PER_EMPLOYEE_ABSTRACT)
- Contingent Worker (ORA_PER_CONTINGENT_WORKER_ABSTRACT)
- Line Manager (ORA_PER_LINE_MANAGER_ABSTRACT)

You can also create 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 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. Aggregate privileges don't inherit other roles. All aggregate privileges are predefined and you can't edit them. Although you can't create aggregate privileges, you can include the predefined aggregate privileges in custom job, abstract, and duty 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 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

When you assign data and abstract roles to users, they inherit all of the data and function security associated with those roles. You can explore the complete structure of a job or an abstract role on the Security Console.

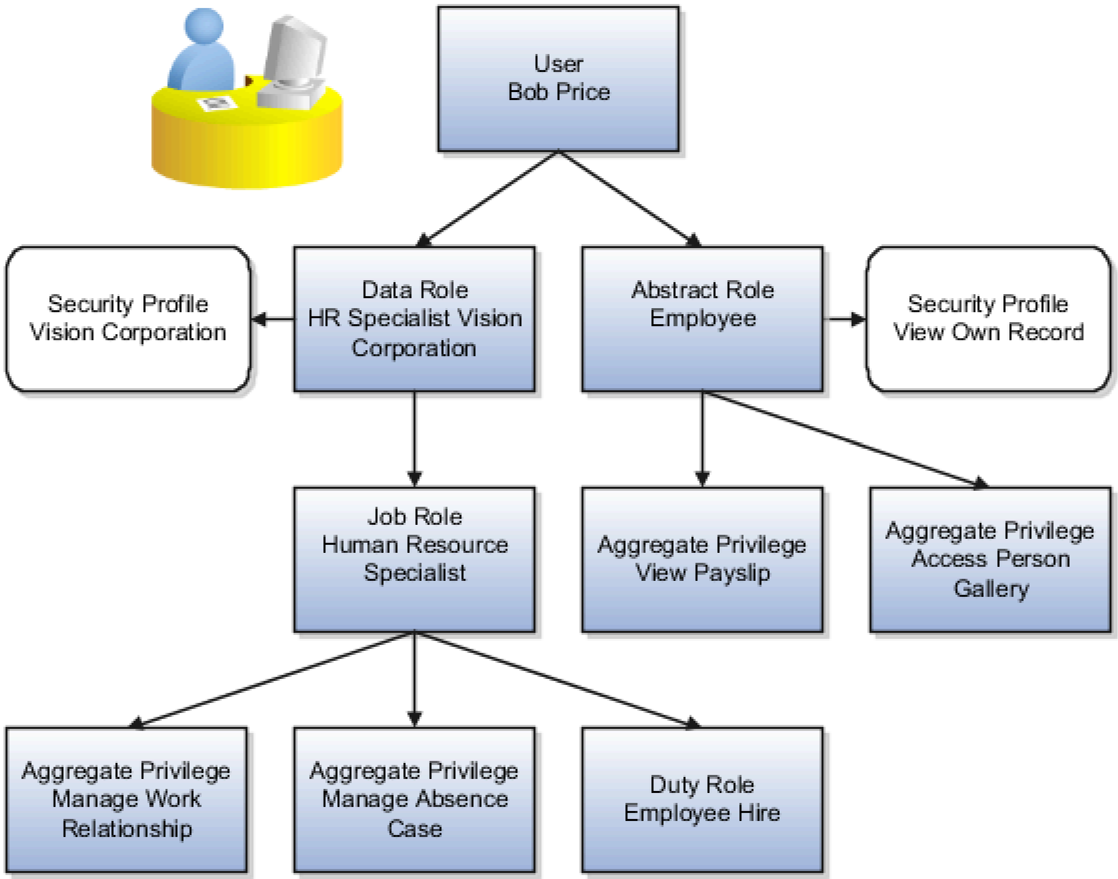
Each role is a hierarchy of other roles:

- HCM data roles inherit job 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.

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

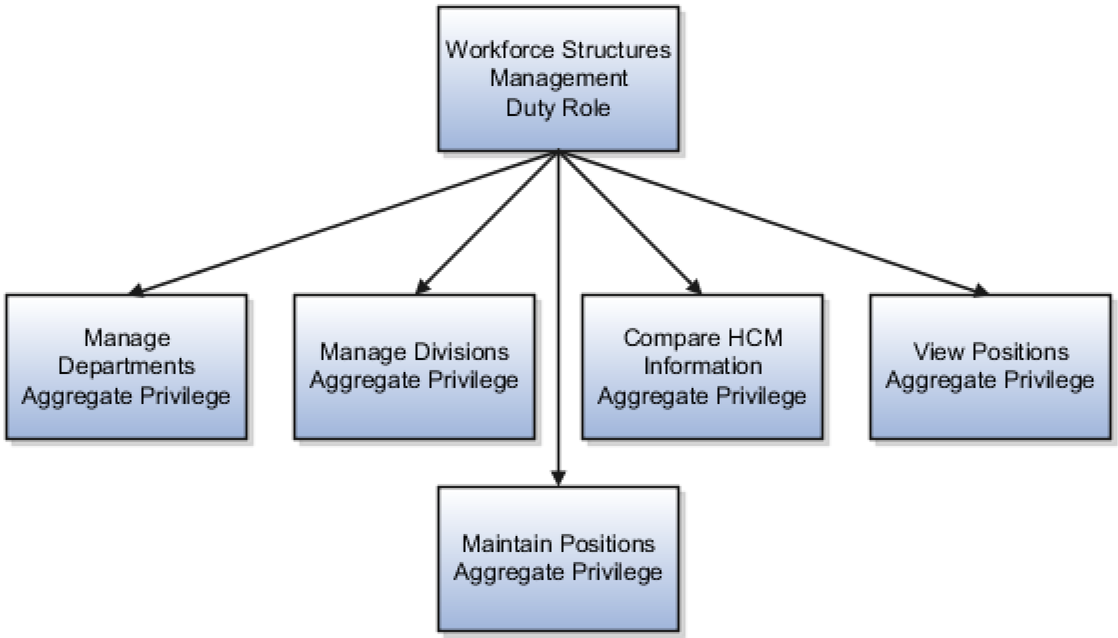
This table describes the two roles.

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 access to secured data 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 access to secured data for the role.

Duty Role Components

This topic describes the components of a typical duty role. You must understand how duty roles are constructed if you plan to create 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 structure shown in this figure.


Workforce Structures Management Duty Role
Manage Departments Aggregate Privilege
Manage Divisions Aggregate Privilege
Compare HCM Information Aggregate Privilege
View Positions Aggregate Privilege
Maintain Positions Aggregate Privilege

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 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

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 might also inherit aggregate privileges. However, aggregate privileges can't inherit other roles of any type. As most function and data security in 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.

Creating, Editing, or Copying 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.

Guidelines for Configuring Security

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 line manager role without those privileges. To create a role, you can either copy an existing role or create a role from scratch.

When you assign predefined roles and privileges as is, you're entrusting users with full access to all data and functionality. Such unrestricted access without really determining the business need might pose a security concern. Also, the assigned privileges might account for subscription consumption irrespective of whether you purchased the cloud service or not. A detailed list of all the predefined roles that impact licensing is available for reference. See the spreadsheet *Predefined Roles with Subscription Impact*.

During implementation, you evaluate the predefined roles and decide whether changes are needed. You can identify predefined roles easily by their role codes, which all have the prefix ORA_. For example, the role code of the Payroll Manager 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. The recommended process is to always make a copy of the predefined role, remove the privileges you don't need, and assign only the required privileges. That way, you will hit the subscription usage in a controlled way, based on your business need. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

> **Note:** Updates to Fusion Applications might also include changes to certain predefined roles. Check the release readiness documents for your product area to know if there are any updates to the predefined roles that are in use. If you find changes that are relevant, incorporate the same changes to your custom role. This will remain an ongoing maintenance activity for the custom roles.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you can create your own 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 can create your own 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 can create your own duty roles. However, the typical implementation doesn't use custom duty roles. You can't create aggregate privileges.

Related Topics

- Options for Reviewing Predefined Roles
- Edit Job Role and Abstract Role
- Create Job Role and Abstract Role from Scratch
- Manage Role Definitions Using CSV File Packages

Options for Reviewing Predefined Roles

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

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.
- Create and manage user categories.
- Manage the default format of user names and the password policy for each user category.
- Manage notifications for user-lifecycle events, such as password expiration, for each user category.
- 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 the Security Console work area. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Create Implementation Users
- Manage Applications Security Preferences
- Manage Duties
- Manage Job Roles

- Revoke Data Role from Implementation Users

2 Creating Implementation Users

HCM Implementation Users

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.

Implementation users can:

- 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.

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 implementation users shown in this table 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 might 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 might 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.

Overview of Creating HCM Implementation Users

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

Sign in to the test or production Oracle HCM Cloud service using the service home URL from the welcome or service-activation email. 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 email. 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 might decide to replace these users or change their definitions. However, these two are required initially.
4	Create Data Roles for Implementation Users	To enable implementation users to access HCM data, you create the following data roles: • HRAnalyst_ViewAll • HCMApplicationAdministrator_ViewAll • HR_Specialist_ViewAll You create additional data roles if you have licensed the Oracle Fusion Workforce Compensation Cloud Service or the Oracle Fusion Global Payroll Cloud Service.
5	Assign Security Profiles to Abstract Roles	Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles. 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.
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.

Related Topics

- Create the TechAdmin Implementation User
- Create the HCMUser Implementation User

Synchronize User and Role Information

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.

Run the Retrieve Latest LDAP Changes Process

Follow these steps:

1. Sign in to your Oracle Applications Cloud service environment as the service administrator.
2. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Initial Users
    - Task: Run User and Roles Synchronization Process
3. On the process submission page for the **Retrieve Latest LDAP Changes** process:
    a. Click **Submit**.
    b. Click **OK** to close the confirmation message.

Import Users and Roles into Applications Security

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.

Run the Import User and Role Application Security Data Process

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

1. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Initial Users
    - Task: Import Users and Roles into Application Security
2. On the Import Users and Roles into Application Security page, click **Submit**.

The **Import User and Role Application Security Data** process starts. When the process completes, you can use the Security Console.

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

Related Topics

- Schedule the Import User and Role Application Security Data Process

Create the TechAdmin Implementation User

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

Create the TechAdmin Implementation User

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

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Initial Users
   - Task: Create Implementation Users
2. On the User Accounts page of the Security Console, click **Add User Account**.
3. Complete the fields on the Add User Account page as shown in the following table.

Field	Value
Associated Person Type	None
User Category	DEFAULT
Last Name	TechAdmin
Email	A valid email 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.

4. Leave the **Active** option selected.

Assign 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. For example, use an HCM data role based on the Human Capital Management Application Administrator role.

Related Topics

- Overview of Creating HCM Implementation Users
- Create the HCMUser Implementation User

Create the HCMUser Implementation User

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

Create the HCMUser Implementation User

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

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Initial Users
   - Task: Create Implementation Users
2. On the User Accounts page of the Security Console, click **Add User Account**.
3. Complete the fields on the Add User Account page as shown in the following table.

Field	Value
Associated Person Type	None

Field	Value
User Category	DEFAULT
Last Name	HCMUser
Email	A valid email 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.

4. Leave the **Active** option selected.

Assign 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. After 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. For example, use an HCM data role based on the Human Capital Management Application Administrator role.

Related Topics

- Overview of Creating HCM Implementation Users
- Create the TechAdmin Implementation User

3 Creating HCM Data Roles for Implementation Users

Overview of HCM Data Roles for Implementation Users

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

Here’s how you can create a data role:

▶ **Watch video**

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

- PayrollAdmin_ViewAll
- PayrollMgr_ViewAll

Related Topics

- Create the HRAnalyst_ViewAll Data Role
- Create the HCMApplicationAdministrator_ViewAll Data Role
- Create the HRSpecialist_ViewAll Data Role
- Create HCM Data Roles for Global Payroll Implementation Users
- Create HCM Data Roles for Workforce Compensation Implementation Users

Create the HRAnalyst_ViewAll Data Role

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.

Create the 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 later.

Follow these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role

   You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
3. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

Field	Value
Data Role Name	HRAnalyst_ViewAll
Job Role	Human Resource Analyst

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

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

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

Related Topics

- Overview of HCM Data Roles for Implementation Users
- Create the HCMApplicationAdministrator_ViewAll Data Role
- Create the HRSpecialist_ViewAll Data Role

Create the HCMApplicationAdministrator_ViewAll Data Role

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.

Create the Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 2. Otherwise, sign in as the TechAdmin user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
    - Functional Area: Users and Security
    - Task: Assign Security Profiles to Role

    You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
3. 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

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

Section	Security Profile
Organization	View All Organizations

Section	Security Profile
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
Transaction	View All HCM Transactions

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

Related Topics

- Overview of HCM Data Roles for Implementation Users
- Create the HRAnalyst_ViewAll Data Role
- Create the HRSpecialist_ViewAll Data Role

Create the HRSpecialist_ViewAll Data Role

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.

Create the Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 2. Otherwise, sign in as the TechAdmin user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:

- Functional Area: Users and Security
- Task: Assign Security Profiles to Role

You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.

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

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

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

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

8. On the Manage Data Roles and Security Profiles page, search for the HRSpecialist_ViewAll data role to confirm that it exists.

Related Topics

- Overview of HCM Data Roles for Implementation Users
- Create the HRAnalyst_ViewAll Data Role
- Create the HCMApplicationAdministrator_ViewAll Data Role

Create the HCMIntegrationSpecialist_ViewAll Data Role

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

Create the Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 2. Otherwise, sign in as the TechAdmin user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role

   You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
3. Complete the fields on the Create Data Role: Select Role page as shown in the following table.

Field	Value
Data Role Name	HCMIntegrationSpecialist_ViewAll
Job Role	Human Capital Management Integration Specialist

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

Section	Security Profile
Organization	View All Organizations
Position	View All Positions

Section	Security Profile
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
Job Requisition	View All Job Requisitions
Candidate	View All Candidates

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

Create HCM Data Roles for Workforce Compensation Implementation Users

If you've licensed the Oracle Fusion Workforce Compensation Cloud Service, then you create the CompensationAdmin_ViewAll and CompensationMgr_ViewAll data roles. You create these roles using the Assign Security Profiles to Role task.

Create the CompensationAdmin_ViewAll Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 2. Otherwise, sign in as the TechAdmin user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role

   You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
3. 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

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

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

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

Create 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
Job Role	Compensation Manager

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

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.

Related Topics

- Overview of HCM Data Roles for Implementation Users

Create HCM Data Roles for Global Payroll Implementation Users

If you've licensed the Oracle Fusion Global Payroll Cloud Service, then you create the PayrollAdmin_ViewAll and PayrollMgr_ViewAll data roles. You create these roles using the Assign Security Profiles to Role task.

Create the PayrollAdmin_ViewAll Data Role

If you're already on the Manage Data Roles and Security Profiles page, then follow this procedure from step 2. Otherwise, sign in as the TechAdmin user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role

   You can also go to this page by selecting **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. In the Search Results section of the Manage Data Roles and Security Profiles page, click **Create**.
3. 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

4. Click **Next**.
5. In the sections of the Create Data Role: Security Criteria page, select the following predefined security profiles for each drop-down list.

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups

Section	Security Profile
Person	View All People
Document Type	View All Document Types
Payroll	View All Payrolls
Payroll Flow	View All Flows

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

Create 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 predefined security profiles shown in this table.

Section	Security Profile
Organization	View All Organizations
Position	View All Positions
Legislative Data Group	View All Legislative Data Groups
Person	View All People

Section	Security Profile
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.

Related Topics

- Overview of HCM Data Roles for Implementation Users

4 Enabling Basic Data Access for Abstract Roles

Why You Assign Security Profiles to Abstract Roles

Users with abstract roles can sign in and open application pages. But they have no automatic access to data. To enable HCM data access for users with abstract roles, you assign security profiles directly to those roles.

These abstract roles are predefined in Oracle HCM Cloud:

- Employee (ORA_PER_EMPLOYEE_ABSTRACT)
- Contingent Worker (ORA_PER_CONTINGENT_WORKER_ABSTRACT)
- Line Manager (ORA_PER_LINE_MANAGER_ABSTRACT)

For example, employees can open the Directory but their searches return no results. Line managers can access My Team functions but can't see data for their organizations.

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.

Related Topics

- Assign Security Profiles to Abstract Roles

Assign Security Profiles to Abstract Roles

In this example, you learn how to assign predefined security profiles to abstract roles during implementation. You perform this task to enable basic data access for the predefined Employee, Contingent Worker, and Line Manager roles.

Search for the Employee Abstract Role

1. Sign in as the TechAdmin user or another user with the IT Security Manager job role or privileges.
2. In the Setup and Maintenance work area, go to the following for your offering:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role
3. On the Manage Data Roles and Security Profiles page, enter **Employee** in the **Role** field. Click **Search**.
4. In the Search Results section, select the predefined **Employee** role and click **Edit**.

Assign 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

Field	Value
LDG Security Profile	View All Legislative Data Groups
Person Security Profile (Person section)	View Own Record
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 the **Assigned** icon appears in the **Security Profiles** column for the Employee role.

   The **Assigned** icon, a 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.

Search 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**.

Assign 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

Field	Value
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
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 the **Assigned** icon appears in the **Security Profiles** column for the Line Manager role.

   The **Assigned** icon confirms that security profiles are assigned to the role.

5 Assigning Roles to Implementation Users

Create a Role Mapping for HCM Implementation Data Roles

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.

Create the Role Mapping

Sign in as the TechAdmin user.

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Manage Role Provisioning Rules
2. In the Search Results section of the Manage Role Mappings page, click **Create**.

   The Create Role Mapping page opens.
3. In the **Mapping Name** field, enter **Requestable Roles**.
4. In the Conditions section, set **HR Assignment Status** to **Active**.
5. In the Associated Roles section, add a row.
6. In the **Role Name** field, search for and select the **HRAnalyst_ViewAll HCM** data role.
7. Select the **Requestable** option.

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

   > **Note:** If **Autoprovision** is selected automatically, then deselect it.
8. Repeat steps 6 and 7 for these roles:
   - HCMApplicationAdministrator_ViewAll
   - HRSpecialist_ViewAll
9. If you created any of the following roles, then repeat steps 6 and 7 for each one:
   - CompensationAdmin_ViewAll
   - CompensationMgr_ViewAll
   - PayrollAdmin_ViewAll
   - PayrollMgr_ViewAll
10. 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.

Assign Abstract and Data Roles to HCMUser

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.

Edit HCMUser

Follow these steps:

1. Sign in as the TechAdmin user.
2. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Initial Users
   - Task: Create Implementation Users
3. On the User Accounts page of the Security Console, search for the HCMUser implementation user.
4. 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:

   - All Users
   - Application Administrator (ORA_FND_APPLICATION_ADMINISTRATOR_JOB)
   - Application Implementation Consultant (ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB)
   - Application Diagnostics Regular User (ORA_FND_DIAG_REGULAR_USER_JOB)
   - Application Diagnostics Viewer (ORA_FND_DIAG_VIEWER_JOB)
5. Click **Edit**.

Assign 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:

   - Contingent Worker
   - Line Manager
   - HRSpecialist_ViewAll
   - HRAnalyst_ViewAll
   - HCMApplicationAdministrator_ViewAll

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

   - CompensationAdmin_ViewAll
   - CompensationMgr_ViewAll
   - PayrollAdmin_ViewAll
   - PayrollMgr_ViewAll

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

   > **Tip:** If you add a role by mistake, you can select it and click **Delete**.

6. Click **Save and Close**.

Verify HCMUser Access

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 in **My Client Groups**, if you use Talent Management.
   - The **Compensation** entry appears in **My Client Groups**, if you use Compensation Management.
   - The **Payroll** entries appear in **Payroll**, 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.

Reset the Cloud Service Administrator Sign-In Details

After setting 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.

Sign in to your Oracle Applications Cloud service using the TechAdmin user name and password and follow these steps:

1. In the Setup and Maintenance work area, go to the following:

    - Functional Area: Initial Users
    - Task: Create Implementation Users

    > **Note:** If you can't see this task, make sure you've selected All Tasks in the **Show** drop-down list.

2. On the User Accounts page of the Security Console, search for your service administrator user name, which is typically your email. Your service activation mail contains this value.
3. In the search results, click your service administrator user name to open the User Account Details page.
4. Click **Edit**.
5. Change the **User Name** value to **ServiceAdmin**.
6. Delete any value in the **First Name** field.
7. Change the value in the **Last Name** field to **ServiceAdmin**.
8. Delete the value in the **Email** field.
9. Click **Save and Close**.
10. 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

Overview of Applications Security Setup Tasks

During implementation the TechAdmin user, who has the IT Security Manager job role, performs the tasks in the Initial Users functional area. This topic introduces some of these tasks. They're described in more detail in this chapter.

Manage Applications Security Preferences

This task opens the Administration tab of the Security Console.

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

- 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.

On the Bridge for Active Directory subtab of the Security Console Administration tab, you configure the bridge for Microsoft Active Directory.

On the User Categories tab of the Security Console, you:

- Create user categories.
- Add users to user categories.
- Specify the default format of user names for the user category.
- Manage the password policy for the user category.
- Manage the notification of user and password events to users in a selected user category.
- Create notification templates for a selected user category.

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. You must also run this process after every release update.

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.

User-Name Formats

During implementation, you specify the default format of user names for the default user category. This topic describes the available formats. To select a format, you perform the Manage Applications Security Preferences task, which opens the Administration page of the Security Console.

Click the **User Categories** tab and click the name of the default user category to open it. Click **Edit** on the **Details** subtab to edit the user-name format. You can change the format for any user category at any time.

Available User-Name Formats

This table describes the available user-name formats.

User-Name Format	Description
Email	The work email (or party email, 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. **Email** is the default format.
FirstName.LastName	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.
FLastName	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.
Person or party number	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.

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

System User Names

The selected user-name rule might fail. For example, a person's party number, person number, or email might 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. Email
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 Email

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

Password Policy

During implementation, you set the password policy for the default user category. This topic describes the available options. To set the password policy, you perform the Manage Applications Security Preferences task, which opens the Administration page of the Security Console.

Click the **User Categories** tab and click the name of the default category to open it. Click **Edit** on the **Password Policy** subtab to edit the policy. You can change the password policy for any user category at any time.

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
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 **Note:** This value is 10 for new installations from Update 18B.
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.	4

Password-Policy Option	Description	Default Value
	If the link expires before the password is reset, then reset must be requested again. You can enter any value between 1 and 9999.	
Password Complexity	Specifies whether passwords must be simple, complex, or very complex. Password validation rules identify passwords that fail the selected complexity test. The following password complexity types are available: • Simple: Must contain at least 8 characters, 1 number. This is the default complexity type. • Complex: Must contain at least 8 characters, 1 uppercase, 1 number. • Very Complex: Must contain at least 8 characters, 1 uppercase, 1 number, 1 special character. • Custom: Provides the flexibility to specify a combination of parameters to define a custom password. By default, the parameters are populated with predefined set of values to get you started. **Note:** For more information about defining custom password, see topic Configure a Custom Password Policy in the Related Topics section	Simple
Disallow last password	Select to ensure that the new password is different from the last password. If the user requests password reset by selecting **Settings and Actions** > **Set Preferences** > **Password**, then this option determines whether the last password can be reused. However, when a user's password expires, the user can reuse the last password. This option doesn't affect password reuse after expiry. This option doesn't take affect the first time a password is reset if a user is moved from a user category that didn’t have the Disallow last password option checked.	No
Administrator can manually reset password	Passwords can be either generated automatically or reset manually by the IT Security Manager. 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 of password events only if appropriate notification templates are enabled for their user categories. The predefined notification templates for these events are Password Expiry Warning Template, Password Expiration Template, and Password Reset Template.

Related Topics

- Configure a Custom Password Policy

Configure a Custom Password Policy

Single Sign-On (SSO) configuration enforces users to use complex passwords. But, some users might want to use simpler passwords that don't enforce the use of minimum number of digits or characters. Using Security Console, you can create a custom password policy for such users.

Since password policies are linked with user categories, you can define a custom password policy for a specific user category. The policy automatically applies all users in that user category. However, there are a few conditions for creating a custom password policy. Users who use an SSO password can't use a custom password because their organization sets the SSO password policy. You can't create a custom password policy using the default Simple, Complex, and Very Complex password complexity options. You must use the Custom option and set values based on your security requirements.

1. On the Security Console, click **User Categories**.
2. Select a user category for which you want to create a custom password policy.
3. Click **Password Policy** > **Edit**.
4. Select **Custom** in the **Password Complexity** drop-down list.
5. Enter the values for all the password parameters as required.
6. Click **Save and Close**.

If you add existing users to the selected user category, then the custom password policy is enforced when they reset their password. If you want to create more custom passwords, then you must create user categories for each custom password.

Role Preferences

During implementation, you set default role preferences for the enterprise. To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration page. Click the Roles subtab of the Administration page.

This topic describes the role preferences and their effects. You can also set role preferences at any time on the Security Console.

Copied-Role Names

To create 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. To limit the number of nodes in the graphical view, set 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, you're recommended to switch to the tabular format.

Related Topics

- Guidelines for Copying HCM Roles
- Graphical and Tabular Role Visualizations

User Categories

You can categorize and segregate users based on the various functional and operational requirements. A user category provides you with an option to group a set of users such that the specified settings apply to everyone in that group.

Typical scenarios in which you may want to group users are:

- Users belong to different organizations within an enterprise and each organization follows a different user management policy.

- Practices related to resetting passwords are not uniform across users.
- Users have different preferences in receiving automated notifications for various tasks they perform in the application.

On the Security Console page, click the User Category tab. You can perform the following tasks:

- Segregate users into categories
- Specify Next URL
- Enable notifications

Segregate Users into Categories

Create user categories and add existing users to them. All existing users are automatically assigned to the Default user category unless otherwise specified. You may create more categories depending upon your requirement and assign users to those categories.

> **Note:** You can assign a user to only one category.

Specify Next URL

Specify a URL to redirect your users to a website or an application instead of going back to the Sign In page, whenever they reset their password. For example, a user places a password reset request and receives an Email for resetting the password. After the new password is authenticated, the user can be directed to a website or application. If nothing is specified, the user is directed to Oracle Applications Cloud Sign In page. You can specify only one URL per user category.

Related Topics

- User-Name and Password Notifications
- Add Users to a User Category
- Using REST API to Add Users to a User Category

Add Users to a User Category

Using the Security Console, you can add existing users to an existing user category or create a new category and add them. When you create new users, they're automatically assigned to the default category.

At a later point, you can edit the user account and update the user category. You can assign a user to only one category.

> **Note:** If you're creating new users using Security Console, you can also assign a user category at the time of creation.

You can add users to a user category in three different ways:

- Create a user category and add users to it
- Add users to an existing user category
- Specify the user category for an existing user

> **Note:** You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can't rename a user category.

Adding Users to a New User Category

To create a user category and add users:

1. On the Security Console, click **User Categories** > **Create**.
2. Click **Edit**, specify the user category details, and click **Save and Close**.
3. Click the Users tab and click **Edit**.
4. On the Users Category: Users page, click **Add**.
5. In the Add Users dialog box, search for and select the user, and click **Add**.
6. Repeat adding users until you have added the required users and click **Done**.
7. Click **Done** on each page until you return to the User Categories page.

Adding Users to an Existing User Category

To add users to an existing user category:

1. On the Security Console, click **User Categories** and click an existing user category to open it.
2. Click the Users tab and click **Edit**.
3. On the Users Category: Users page, click **Add**.
4. On the Add Users dialog box, search for and select the user, and click **Add**.
5. Repeat adding users until you have added the required users and click **Done**.
6. Click **Done** on each page until you return to the User Categories page.

Specifying the User Category for an Existing User

To add an existing user to a user category:

1. On the Security Console, click **Users**.
2. Search for and select the user for whom you want to specify the user category.
3. On the User Account Details page, click **Edit**.
4. In the User Information section, select the **User Category**. The Default user category remains set for a user until you change it.
5. Click **Save and Close**.
6. On the User Account Details page, click **Done**.

You can delete user categories if you don't require them. However, you must ensure that no user is associated with that user category. Otherwise, you can't proceed with the delete task. On the User Categories page, click the **X** icon in the row to delete the user category.

User-Name and Password Notifications

By default, users in all user categories 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 templates for any user category.

During implementation, you identify the notifications that you plan to use for each user category 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 these notification templates and their associated events on the User Category: Notifications page of the Security Console for a user category.

Template Name	Description	Sent to Inactive Users?	Sent to Locked Users?
ORA Administration Activity Request	Notifies the user when an administrator initiates an administration activity	Yes	Yes
ORA Expiring External IDP Signing Certificate	Warns the user that an external identity provider certificate is expiring soon	No	Yes
ORA Expiring Service Provider Encryption Certificate	Warns the user that a service provider encryption certificate is expiring soon	No	Yes
ORA Expiring Service Provider Signing Certificate	Warns the user that a service provider signing certificate is expiring soon	No	Yes
ORA Forgot User Name	Sends the user name to a user who requested the reminder	No	Yes
ORA Location Based Access Disabled Confirmation	Notifies the user when an administrator disables location-based access through an administration activity request	Yes	Yes
ORA New Account	Notifies a user when a user account is created and provides a reset-password link	Yes	Yes
ORA New Account Manager	Notifies the user's manager when a user account is created	Yes	Yes
ORA Password Generated	Notifies the user that a password has been generated automatically and provides instructions for resetting the password	Yes	Yes
ORA Password Expiration	Notifies the user that a password has expired and provides	No	No

Template Name	Description	Sent to Inactive Users?	Sent to Locked Users?
	instructions for resetting the password		
ORA Password Expiry Warning	Warns the user that a password is expiring soon and provides instructions for resetting the password	No	No
ORA Password Reset	Sends a reset-password link to a user who performed the Reset Password action on the My Account page	No	Yes
ORA Password Reset Confirmation	Notifies the user when a password has been reset	No	Yes
ORA Password Reset Manager	Sends a reset-password link to the manager of a user who performed the Reset Password action on the My Account page	No	Yes
ORA Password Reset Manager Confirmation	Notifies the user's manager when a user's password has been reset	No	Yes
ORA Single Sign-On Disabled Confirmation	Notifies the user when an administrator disables Single Sign-On through an administration activity request	Yes	Yes

When you create a user category, it's associated automatically with the predefined notification templates, which are all enabled. You can update user categories using the SCIM API, and you can perform bulk updates to categories using HCM Data Loader. For information on adding users to a user category, see the topic Add Users to a User Category.

You can't edit or delete predefined notification templates that begin with the prefix ORA. You can only enable or disable them. However, you can update or delete the user-defined templates. Each predefined event can be associated with only one enabled notification template at a time.

> **Note:** Both pending workers and terminated workers receive emails at their personal email address.

Enabling and Disabling Notifications

For any notification to be sent to the users in a user category, notifications in general must be enabled for the user category. Ensure that the **Enable notifications** option on the User Category: Notifications page is selected. When notifications are enabled, you can disable specific templates. For example, if you disable the New Account Template, then users in the relevant user category aren't notified when their accounts are created. Other notifications continue to be sent.

To disable a template:

1. Click **Edit** on the User Category: Notifications page.

2. In edit mode, click the template name.
3. In the template dialog box, deselect the **Enabled** option.
4. Click **Save and Close**.

Related Topics

- Add Users to a User Category

How can I enable notifications for pending workers?

You can send notifications to the personal email address of pending workers and terminated workers. To send the notification, you must enable the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option.

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, search for and select the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option code.
3. In the Profile Values section, enter **Y** as the profile value.
4. Click **Save and Close**.

Why don't I see my user name in the forgot password email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

Why don't I see my user name in the forgot user name email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

Create a Notification Template

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 your own notifications, you create notification templates.

Follow these steps to create a notification template:

1. Open the Security Console and click the User Categories tab.

2. On the User Categories page, click the name of the relevant user category.
3. On the User Categories: Details page, click the Notifications subtab.
4. On the User Category: Notifications page, click **Edit**.
5. Click **Add Template**.
6. In the Add Notification Template dialog box:

    a. Enter the template name.
    b. 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.
    c. Update the **Message Subject** field, as required. The text that you enter here appears in the subject line of the notification email.
    d. Update the message text, as required.

    This table shows the tokens supported in the message text.

Token	Meaning	Events
userLoginId	User name	- Forgot user name - Password expired - Password reset confirmation - New account created
firstName	User's first name	All events
lastName	User's last name	All events
managerFirstName	Manager's first name	- New account created - manager - Password reset confirmation - manager - Password reset - manager
managerLastName	Manager's last name	- New account created - manager - Password reset confirmation - manager - Password reset - manager
loginURL	URL where the user can sign in	- Expiring external IDP signing certificate - Password expired - Password expiry warning
resetURL	URL where the users can reset their password	- New account created - manager - New user created - Password generated - Password reset - Password reset - manager
CRLFX	New line	All events

Token	Meaning	Events
SP4	Four spaces	All events
adminActivityUrl	URL where an administrator initiates an administration activity	Administration activity requested
providerName	External identity provider	Expiring external IDP signing certificate
signingCertDN	Signing certificate	Expiring external IDP signing certificate
signingCertExpiration	Signing certificate expiration date	- Expiring external IDP signing certificate - Expiring service provider signing certificate
encryptionCertExpiration	Encryption certificate expiration date	Expiring service provider encryption certificate
adminFirstName	Administrator's first name	- Administration activity location-based access disabled confirmation - Administration activity single sign-on disabled confirmation
adminLastName	Administrator's last name	- Administration activity location-based access disabled confirmation - Administration activity single sign-on disabled confirmation

    e. To enable the template, select the **Enabled** option.
    f. Click **Save and Close**.

7. Click **Save** on the User Category: Notifications page.

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

Schedule the Import User and Role Application Security Data Process

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.

The process 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 the **Import User and Role Application Security Data** process 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.

Schedule the Process

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

1. 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 **Days Between Runs** 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.

Review 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.

Schedule the Import User Login History Process

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 the **Import User Login History** task 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.

Schedule the Process

Follow these steps:

1. 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

Why You Should Run the Send Pending LDAP Requests Process

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 emails.

  If you include work emails when you create person records, then the process sends those emails 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 Fusion Cloud HCM.

> **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.

Schedule the Send Pending LDAP Requests Process

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. After you schedule the process you can't run it on an as-needed basis, which may be necessary during implementation.

Schedule the Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
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**.

Related Topics

- Why You Should Run the Send Pending LDAP Requests Process

Retrieve Latest LDAP Changes

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. You're also recommended to run this process after any release update.

Run the Process

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

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.

   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.

7 Managing Location-Based Access

Overview of Location-Based Access

You can use location-based access to control user access to tasks and data based on their roles and computer IP addresses.

To enable location-based access and make a role public, you must have the IT Security Manager role. You can make a role public only when location-based access is enabled. To enable location-based access, you must register the IP addresses of computers from which the users usually sign in to the application.

Let's take an example to understand how location-based access is useful. You want your users to have complete access to tasks or features when they're signed in to the application from your office network. But you want to restrict the access if the users are signing in from a home computer or an internet kiosk. To control the user access, you must enable location-based access and register the IP addresses of your office computers on the Security Console. Users have complete access to the tasks or features if they sign in from office computers. If they sign in to the application from an unregistered computer, they can view and access only the generic tasks that aren't tied to any particular role. From an unregistered computer, they can't access the role-based tasks, which they could access from office.

What Happens When You Enable Location-Based Access

When you enable location-based access, users who sign in to the application from registered IP addresses have complete access to all tasks. On the other hand, users signing in from unregistered IP addresses have no access to their role-based tasks and data. However, you can grant complete access to these users too, when required. You can also grant public access (access from all IP addresses) to certain roles. The users associated with those roles can access all tasks, no matter which IP address they sign in from.

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email
- The IT Security Manager role
- Email notifications are enabled

Related Topics

- How Location-Based Access Works
- Enable and Disable Location-Based Access

How Location-Based Access Works

Location-based access combines the registered IP addresses of the computers and public roles to control access to the application.

Scenarios

To understand how location-based access works, consider the following scenarios and their effect on user access.

To avoid any access-related issue, carefully examine the given scenarios and plan well before you enable location-based access.

Scenario	Impact on User Access
You disable location-based access.	All users signing into the application from their respective computers continue to have the same level of access as they had earlier.
You enable location-based access and register few IP addresses, but don't grant public access to any role.	• Users who sign into the application from the registered IP addresses have access to their tasks as usual. • Users signing in from unregistered IP addresses can access only the generic tasks that aren't tied to any particular role.
You enable location-based access, register a few IP addresses, and grant public access to certain roles.	• Users signing in from the registered IP addresses have complete access. • Users signing in from unregistered IP addresses can't access any role-based tasks unless you grant public access to those roles. If you have made a role public, users can access all the tasks tied to that role.
You enable location-based access, but don't register any valid IP address, and don't grant public access to any role.	Users can sign in with valid credentials but can access only the generic tasks that aren't assigned to a specific role. **CAUTION:** Try and avoid this scenario. Register at least one valid IP address and grant public access (access from all IP addresses) to IT Security Manager role when you enable location-based access.

Related Topics

- How can I make a role public?
- How can I ensure that I always have access to the Security Console?

Enable and Disable Location-Based Access

You can enable location-based access so that you can allow users to access tasks and data based on their roles and registered IP addresses. By default, location-based access is disabled.

Before You Start

Configure location-based access in a test environment and try it out before you configure it in a production environment. You must have the IT Security Manager role to enable location-based access. Additionally, you must:

- Set up a valid email address. When required, the location-based access control reset or recovery notification is sent to that email address.

- Add yourself to the user category for which the notification template **ORA Administration Activity Request Template** is enabled.
- Keep the list of valid IP addresses ready.

Enable Location-Based Access

1. Click **Navigator** > **Tools** > **Security Console**.
2. On the Administration page, click the Location Based Access tab.
3. Select **Enable Location Based Access**.
4. In the **IP Address Allowlist** text box, enter one or more IP addresses separated by commas. For example, 192.168.10.12, 192.168.10.0. To indicate a range of IP addresses, you may follow the Classless Inter-Domain Routing (CIDR) notation, such as 192.168.10.0/24.

   > **Note:** You can enter the IP address (IPv4 only) range suffix only up to 32 in the **IP Address Allowlist** text box. For example, 168.1.192.0/32 to 168.1.192.32/32.

   > **Tip:** Your computer's IP address appears on the page. Add that IP address to the list so that your access to the application remains unaffected when you sign in from that computer.

5. Click **Save**.
6. Review the confirmation message and click **OK**.

After you enable location-based access, make the IT Security Manager's role public to access Security Console even from an unregistered IP address.

Disable Location-Based Access

To disable location-based access, deselect the **Enable Location Based Access** check box. The existing IP addresses remain in a read-only state so that you can reuse the same information when you enable the functionality again. At that point, you can add or remove IP addresses based on your need.

Related Topics

- What is allowlisting?
- Why can't I see the Location Based Access tab on the Administration page?

Examples of Location-Based Access in Oracle HCM Cloud

This topic describes some typical use cases for creating public roles for Oracle HCM Cloud users. Using these roles, users can perform a restricted set of tasks from IP addresses that aren't registered.

Public Access for Pending Workers

During preboarding, pending workers may need to complete some tasks in Oracle HCM Cloud. Pending workers can't usually access the office network or use registered IP addresses. So, to let them complete tasks such as viewing personal information or uploading document records, you can make the Pending Worker role public. Or, to limit what the Pending Worker role can do, you could create a custom role with limited privileges and make it public. Pending workers could then complete their preboarding tasks when signed in from any IP address.

Public Access for External Learners

Let's say that you need to let external learners, such as partners, resellers, contractors, or franchisees, complete some company training. Usually, only employees can access learning, and they need to be in the office network or using a registered IP address. To let external learners use selected learning tasks, you could create an External Learner role and make it public. The role would support just the tasks that external learners need. Users with the External Learner role could then access learning from any IP address.

Public Access for Oracle Recruiting Cloud Users

Suppose that all external candidates need to access Oracle Recruiting Cloud career sites from the public domain. To give them this access, you can make the predefined Anonymous User abstract role (ORA_FND_ANONYMOUS_USER_ABSTRACT) public.

Any integrations with approved third-party party vendors use REST APIs to send data back to Oracle Recruiting Cloud. To support these integrations, you can create a custom integration role with integration privileges. You may need more than one of these roles, depending on the integration services, such as job distribution, background check, and assessments, that you enabled. You would need to make all of the custom roles public, so that the REST APIs can be called by partner applications outside your intranet. You would also have to give the integration roles to the Oracle Recruiting Cloud users who start the integration request from the application. Oracle Recruiting Cloud doesn't provide predefined.integration roles.

Related Topics

- Integrating Third Party Services
- Set Up Partner Integration Provisioning

FAQs for Managing Location-Based Access

What is allowlisting?

Allowlisting is the process of granting trusted entities access to data or applications. When you enable location-based access and register the IP addresses of computers, you're storing those IP addresses as trusted points of access.

You can include IP Addresses of all computers hosting cloud applications (both Oracle and non-Oracle) that require access to Oracle Applications Cloud. In other words, you're allowlisting those IP addresses. Users signing in from those computers are considered as trusted users and have unrestricted access to the application.

Why can't I see the Location Based Access tab on the Administration page?

To prevent any incorrect configuration, the profile option Enable Access to Location Based Access Control associated with the Location Based Access tab is perhaps disabled. As a result, the tab isn't visible.

Contact your Application Implementation Consultant or Administrator to enable the profile option so that the Location Based Access tab appears on the Administration page.

How can I make a role public?

On the Security Console, identify the role that you want to make public. Except duty roles, you can make all roles public. On the Edit Role page, select the option Enable Role for Access from All IP Addresses and save the changes.

> **Note:** You can make a role public only if location based access is enabled.

How can I ensure that I always have access to the Security Console?

If location-based access is enabled, you must add your computer's IP address to the allowlist. Also ensure that the IT Security Manager role is granted public access.

Even if you have to sign in from an unregistered computer, you can still access the Security Console and other tasks associated with the IT Security Manager role.

How can I disable Location-based Access when I am not signed in to the application?

You want to disable location-based access but you're locked out of the application and can't sign in to the Security Console. You must request access to the Administration Activity page using the URL provided to the administrators.

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Location Based Access** option and click **Submit**. You receive a confirmation that location-based access is disabled. Immediately, you're redirected to the Oracle Applications Cloud page where you can sign in using your registered user name and password, and gain access to tasks and data as earlier.

8 Single Sign-On

Oracle Applications Cloud as the Single Sign-On (SSO) Service Provider

Your users are likely to access different internal and external applications to perform their tasks. They might require access to different applications hosted by partners, vendors, and suppliers.

Certainly, users won't like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.

Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

Initial Sign-in

On a typical working day, when users sign in for the first time, they request access to an application or a web page. Oracle Applications Cloud, which is set up as a service provider, sends a verification request to the user's identity provider who's already added to the Security Console. The identity provider verifies the user credentials and sends the authorization and authentication response back to the service provider. After successful authentication, users are granted access to the required application or web page. Because the authentication is valid across your enterprise network, users don't have to sign in again when accessing different applications available on the same network. This entire trust chain between the service provider and the various identity providers is established using the Security Assertion Markup Language (SAML) 2.0 standards.

Final Sign-out

Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they're automatically signed out from all applications on the network. This is to prevent unauthorized access and to ensure that data remains secure all the time.

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email
- The IT Security Manager role
- Email notifications are enabled

Configure Single Sign-On

To enable single sign-on in your environment, complete the settings in the Single Sign-on Configuration section on the Security Console. This configuration lets you enable a login page and a page to which users must be redirected to after logging out of the application.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. In the Single Sign-On Configuration section, click **Edit**.
3. Enter the **Sign Out URL**. Users are redirected to this page once they sign out from the application.

   > **Note:** The Sign Out URL is the same for all the identity providers that you configure.

4. If **Enable Chooser Login Page** isn't enabled already, select it to display the service provider's single sign-on page along with your company's login page.
5. Click **Save**.

To configure Oracle Applications Cloud as the service provider, you must do the following:

- Review the service provider details
- Add an identity provider
- Test the identity provider
- Enable the identity provider

On the Security Console, go to the Single Sign-On tab and click **Create Identity Provider**.

> **Note:** Oracle Cloud Applications support all SAML 2.0 compatible federation servers.

Review Service Provider Details

- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

You must share these details with the identity providers so that they can use them to configure your application as the associated service provider.

Add an Identity Provider

You can add as many identity providers as required to facilitate single sign-on for all your users. However, one of them must be the default identity provider.

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn't complete.

> **Note:** Including encryption certificate in the metadata file is optional.

1. On the Security Console, click **Single Sign-On** > **Create Identity Provider**.
2. On the Identity Provider Details page, click **Edit** and enter the identity provider details:
   - Provide a **Name** and **Description** for the identity provider. Ensure that the identity provider name is unique for the partnership.
   - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select **Email**. Otherwise, leave it as **Unspecified**.
   - Enter the **Relay State URL**. Users are directed to this URL to sign and authenticate irrespective of which application they want to access.
   - Select the **Default Identity Provider** check box to make this identity provider the default one.
3. Import the identity provider metadata:
   - If it's an XML file, click **Browse** and select it.
   - If it's available on a web page, select the **External URL** check box and enter the URL. External URL isn't stored in this configuration and is used only for importing the identity provider metadata during identity provider creation or modification.

   > **Note:** The metadata XML file must be Base64 encoded.

4. Click **Save and Close**.

   > **Note:** Oracle Applications Cloud can't be used as an identity provider.

Test the Identity Provider

Click the Diagnostics and Activation tab to verify if the identity provider that you added works as expected.

1. Click the **Test** button to run the diagnostics. The Initiate Federation SSO page appears.
2. Click the **Start SSO** button. You're prompted to enter the user credentials of any user registered with the identity provider. The test validates whether the federation single sign-on is successful or not. The result summary includes the following details:
   - Status of authentication: success or failure
   - The attributes passed in the assertion
   - The assertion message in XML

You can review the log messages that appear in the Federation Logs section to identify if there are any configuration issues with the identity provider.

> **Note:** You must run the test whenever there's a change in the identity provider configuration.

Enable the Identity Provider

If everything looks fine, you can go ahead and enable the identity provider. While you're on the Diagnostics and Activation page, click **Edit** and select the **Enable Identity Provider** check box. The identity provider is now active.

> **Note:** You can enable an identity provider only after you import service provider metadata into the identity provider.

FAQs for Single Sign-On

Does the service provider store user passwords?

No. Passwords are stored with the identity providers. When a user signs in, the identity provider authenticates the password, authorizes the request to access an application, and sends that confirmation back to the service provider.

The service provider then allows users to access the application or web page.

Can I set up an identity provider without enabling it?

Yes, you can set up an identity provider and test it thoroughly before enabling it. By default, an identity provider remains disabled. You can disable an identity provider at any time.

How can I allow my users to sign in using their company's credentials?

On the Security Console, go to Single Sign-On Identity Provider Details page and make sure that the Enable Chooser Login Page check box is selected.

When your users access the main portal page, they can sign in using one of the following options:

- The single sign-on credentials registered with the identity provider
- The single sign-on credentials registered with their company

What should I do to extend the validity of certificates provided by the identity provider?

Pay attention to the notifications you receive about certificate expiry. Request your identity provider to share with you the updated metadata file containing renewed certificate validity details.

Once you upload the metadata file, the validity of the certificate is automatically renewed. You will have to monitor this information at intervals to ensure that the certificates remain valid at all times.

How can the identity provider obtain renewed certificates from the service provider?

The identity provider can submit a service request to the service provider asking for the renewed signing and encryption certificates.

How can I disable Single Sign-On when I am not signed in to the application?

You must request access to the Administration Activity page using the URL provided to the administrators.

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Single Sign On** option and click **Submit**. You receive a confirmation that single sign-on is disabled. Immediately, you're redirected to the Oracle Applications Cloud page where you can sign in using your registered user name and password.

What are the different events and notifications associated with the Single Sign-On functionality?

Automatic notifications are sent for the following events associated with single sign-on.

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled using the Administration Activity page, notification is sent to that user who disabled SSO.
- When the external identity provider's signing certificate is about to expire
- When the service provider's signing certificate is about to expire
- When the service provider's encryption certificate is about to expire

Note: Notifications are sent to users who are assigned the **Administer SSO** (ASE_ADMINISTER_SSO_PRIV) privilege,according to the following schedule:

- First notification - 60 days before the expiry date
- Second notification - 30 days before the expiry date
- Last notification - 10 days before the expiry date.

9 API Authentication

Configure Inbound Authentication

Third-party application users can access a service of Oracle Applications Cloud if inbound authentication is configured for them. You can use an Oracle API Authentication Provider to configure inbound authentication for such users.

To configure inbound authentication, you need a public certificate and a trusted issuer which contains the tokens.

Oracle Applications Cloud supports the JSON Web Token (JWT), Security Assertion Markup Language (SAML), and Security Token Service (STS) tokens. Use the Security Console to configure the trusted issuer and public certificate details. The default trusted issuer is Oracle (www.oracle.com) and you can't delete it.

We recommend that you use JWT for inbound authentication for a system account that's created for a specific application. For authentication, JWT uses a combination of a public certificate and trusted issuer whereas a system account's password expires soon based on the security policy. In addition, you must ensure that the system account's credentials are valid.

> **Note:** For more information about how to configure a JWT for inbound authentication, see Configure JWT Authentication Provider in the Related Topics section.

How Inbound Authentication Works

When a third-party application user sends an authentication request to access a service of Oracle Applications Cloud, these actions occur in the background:

1. The third-party application generates a JWT that includes trusted issuer and public certificate information.
2. Oracle Web Services Manager authenticates the generated JWT by verifying whether the trusted issuer and public certificate are valid.
3. On successful authentication, the third-party application gets access to the Oracle Applications Cloud service.

Here's how you configure an Oracle API Authentication Provider for inbound authentication:

1. On the Security Console, click **API Authentication**.
2. Click **Create Oracle API Authentication Provider**.
3. On the Oracle API Authentication Provider Details page, click **Edit**.
4. On the API Authentication Configuration Details page, enter a name for the **Trusted Issuer**. Ensure that the name of Trusted Issuer matches the value of ISS in the JWT token.
5. Select one or more token types that you want to include in the trusted issuer.
6. Click **Save and Close**.
7. On the Oracle API Authentication Provider Details page, click the Inbound API Authentication Public Certificates tab and click **Edit**. You can use the default Oracle public certificate or add a new one.
8. On the Inbound API Authentication Public Certificates page, click **Add New Certificate** to add a different public certificate.
9. Enter the **Certificate Alias** name
10. Click **Browse** and select the public certificate that you want to import.

    > **Note:** If the public certificate includes a certificate chain then import the complete chain.

11. Click **Save**. The newly added certificate alias is displayed on the Inbound API Authentication Public Certificates page.
12. Click **Done** to return to the API Authentication page.

Related Topics

- Configure JWT Authentication Provider
- Reset User Password
- Use JSON Web Token for Authorization

Configure Outbound API Authentication Using JWT Custom Claims

A system account is an account used for integrating Oracle Applications Cloud with third-party applications. This account isn't associated with a user but it must have roles with access to REST APIs.

System account uses basic authentication to authenticate users even if single sign-on is enabled. Security Console's password policy applies to a system account and so the password of this account expires based on the password policy.

Critical tasks such as batch operations or data synchronizations must continue without any interruption or the need to re-authenticate at intervals. To support such tasks, you need to define custom parameters for authentication. Using Security Console, you can define a JSON Web Token (JWT) that can be used by REST APIs to automate system authentication without you having to authenticate manually.

JWT is an access token that contains custom claim name and claim values. Custom claims are name and value pairs that you can define in a JWT. To uniquely identify a user, you can add the user's email address to the token along with the standard user name and password.

Example, suppose you want to integrate Oracle Applications Cloud with a third-party application. This integration uses the JWT Custom Claims to authenticate the users who sign into Oracle Applications Cloud to access the third-party application.

Do these steps to define a JWT that will be used for integration with third-party application:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**, **Edit**.
3. Enter a name and description for the external client application that you want to create.
4. In the **Select Client Type** drop-down list, select **JWT Custom Claims** and click **Save and Close**.
5. Click the JWT Custom Claims Details tab and click **Edit**.
6. In the Token Settings section, if required, update the **Token Expiration Time** and **Signing Algorithm**. Default values are 30 minutes and RS256 respectively.
7. Click **Save**.
8. In the JWT Custom Claims section, click **Add**. You can either select a name from the predefined values in the drop-down list or select **Other** and enter a name of your choice.
9. Select a value for the custom claim. If you select **Free-form**, enter the value in the following text box. You can add more JWT custom claims using the **Add** button.
10. Click **Save**. You can add more parameters as required.
11. Click **Done** to return to the JWT Custom Claims Details page.

    You can view the token created for authentication using the **View JWT** button on the JWT Custom Claims Details page. The View JWT window displays the header and payload of the JWT.

12. Click **Done** again to return to the API Authentication page. You can view the newly created JWT Custom Claim in this page.

You can delete a JWT custom claim on the API Authentication page.

Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol

OAuth is an open industry standard protocol that allows applications access information from other third-party applications, on behalf of the users. The OAuth authorization protocol manages access securely without revealing any passwords to the client application, such as Oracle Applications Cloud.

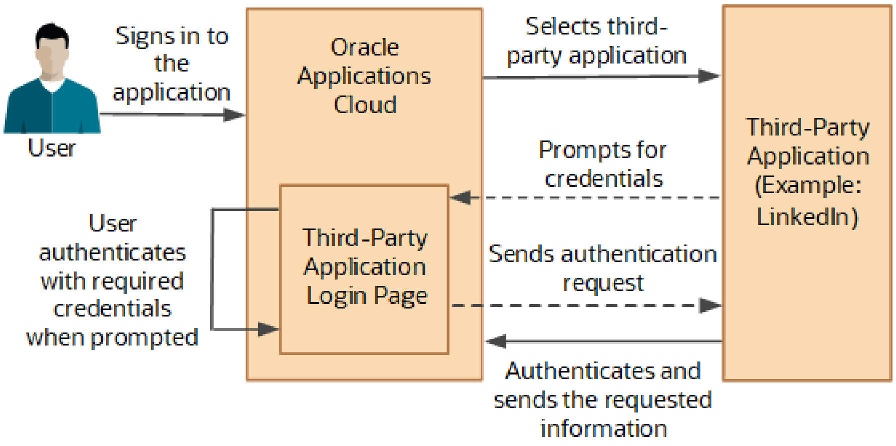
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required permissions to Oracle Applications Cloud to access the information from LinkedIn.

As you notice, there are three parties involved in the entire authentication process: Oracle Applications Cloud, the user who owns information on LinkedIn, and LinkedIn's authorization server. This authorization protocol always requires three such parties for the authentication to complete. Therefore, this protocol is called three-legged OAuth authorization protocol.

Here's the sequential representation of the end-to-end authorization process between Oracle Applications Cloud and the LinkedIn server:

1. Oracle Applications Cloud registers the Client ID and Client Secret and other settings required for authorization.
2. When an Oracle Applications Cloud user wants to access profile information, the LinkedIn login page appears, where the user authenticates using the required credentials.
3. On successful authentication, LinkedIn's authorization server sends an authorization code to Oracle Applications Cloud.
4. Oracle Applications Cloud receives the authorization code and sends an access token request to LinkedIn. LinkedIn processes the access token request and returns an access token.
5. Oracle Applications Cloud uses the access token to call LinkedIn APIs on behalf of the user to access the required information. At runtime, Oracle Web Services Manager manages the entire authorization process.

The following graphic shows the entire authorization process between Oracle Applications Cloud and the LinkedIn server:


User
Signs in to the application
Oracle Applications Cloud
Selects third-party application
Third-Party Application (Example: LinkedIn)
Prompts for credentials
User authenticates with required credentials when prompted
Third-Party Application Login Page
Sends authentication request
Authenticates and sends the requested information

Using the Security Console, you configure the three-legged OAuth authorization settings for Oracle Applications Cloud. Once configured, users can access their information from a third-party application, within Oracle Applications Cloud.

Before you proceed, you must enable a profile option to get the OAuth Three-Legged option on the External Client Applications Details page. See the Related Information section for more information.

Here's how you configure three-legged OAuth authorization:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**.
3. On the External Client Application Details page, click **Edit**.
4. Enter a name and description for the external client application that you want to create.
5. In the **Select Client Type** drop-down list, select **OAuth Three-Legged**.
6. Click **Save and Close** to return to the External Client Application Details page.
7. Click the OAuth Details tab.
8. On the Three-Legged OAuth Details page, click **Edit**.
9. Enter the appropriate values in the following required fields:
    - Authorization URL - The authorization code link that the authorization server sends to the application.
    - Redirect URL - The page to which the user is redirected to after successful authorization of application.
    - Access Token URL - The access token that's sent from the authorization server to the application.
    - Servlet Application URL - The access token that's sent from the authorization server to the application.
    - Client ID - The access token that's sent from the authorization server to the application.
    - Client Secret - The access token that's sent from the authorization server to the application.
    - Client Scope - The access token that's sent from the authorization server to the application.
10. Enter the appropriate values in the following optional fields, if required:
    - Server Scope - The access token that's sent from the authorization server to the application.
    - Federated Client Token - The access token that's sent from the authorization server to the application.
    - Include Client Credential - The access token that's sent from the authorization server to the application.
    - Client Credential Type - The access token that's sent from the authorization server to the application.
11. Click **Save and Close**.
12. Click **Done** to return to the Three-Legged OAuth Details page.
13. Click **Done** again to return to the API Authentication page. You can view the newly created three-legged OAuth configuration here.

Related Topics

- Enable OAuth Three-Legged Authentication for Creating External Client Application

Enable OAuth Three-Legged Authentication for Creating External Client Application

While creating an external client application using the Security Console, only the JWT custom claims authentication type is available in the Select Client Type list on the External Client Application Details page.

To display the OAuth three-legged authentication type for selection, you must enable it using a profile option.

Here are the steps:

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.
2. Search for the **ORA_ASE_ENABLE_OAUTH_THREE_LEGGED_SETUP** profile option code
3. In the Profile Values section, click the **Profile Values** list for the Site profile level and select Yes.
4. Click **Save and Close**.

The OAuth three-legged authentication type is enabled now. Enabling the profile option displays the OAuth three-legged authentication type in the Select Client Type list on the External Client Application Details page.

Is there a recommended format for the public certificate?

Yes. Oracle recommends that the public certificate you upload must contain only line feed (denoted by the code \n) to indicate separation of lines. Because carriage return isn't supported, make sure that the certificate doesn't contain carriage return along with the line feeds.

10 Export and Import of Security Setup Data

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV export and import functionality.

Let's assume you have spent lot of time and effort in configuring and setting up the Security Console in your primary environment. You test the setup and find that everything's working as intended. Now, you want to replicate the same setup in another environment. And you want that to happen with the least effort and as quickly as possible. Well, it certainly can be done in a simple and less time-consuming way.

In the Setup and Maintenance work area, use the **Manage Application Security Preferences** task in the Initial Users functional area.

Before You Begin

Learn how to export business object data to a CSV file and to import business data from a CSV file. Detailed instructions are available in the *Export and Import CSV File Packages* topic of the Using Functional Setup Manager guide.

What Gets Exported and Imported

The Security Console setup data comprises information that you see on the Administration and User Categories tabs of the Security Console. The following business objects help in packaging those details into CSV files so that the data can be easily exported and imported.

- Security Console Administration Settings
- Security Console User Category
- Security Console User Category Notifications

> **Note:**
> - Lists of users or information about any specific user is never a part of the CSV file.
> - After exporting the setup data to a CSV file, if you want to remove any memberships in the target environment, you must make those changes in the exported CSV file before beginning the import process. Only then, you can apply those changes to the target environment. If you make changes to the source environment alone, you can't expect the CSV file to be automatically updated with memberships that were removed. This is because there's no automatic synchronization between the source environment and the exported CSV file. So, if you don't manually update the CSV file, the changes won't reflect in the target environment.

In this table, you will find information about the contents of each business object.

Business Object	Information Included in Export and Import
Security Console Administration Settings	• General administration details • Role preferences • Location-based access settings • If location-based access isn't enabled (if the tab doesn't appear on Security Console), nothing gets included in the export or import.
Security Console User Category	• User category details • Password policy information
Security Console User Category Notifications	Notification preferences. For notifications, only the custom template information is exported from the default user category. The predefined notifications are excluded because they're available in the target environment.

> **Note:** When you export Security Console setup data, user categories with a password policy configured with custom password complexity setting are exported with the simple password complexity setting. You must manually configure a custom password policy in the new environment with the values used earlier to create it.

When the export process successfully completes, you get the following CSV files:

- Administration Settings CSV
- User Category CSV
- User Category Notifications CSV

If there are language packs installed on your application, additional CSV files may be generated containing the translated data.

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

Related Topics

- Export and Import CSV File Packages
- Key Information About Setup Data Export and Import Processes

Export and Import of HCM Custom Roles and Security Profiles

You're looking at migrating your HCM custom roles, data roles, and security profiles from one environment to another. To accomplish most of your HCM security migration needs, export the business objects in the Users and Security functional area within the Workforce Deployment offering.

Other offerings have a Users and Security functional area, but only the Workforce Deployment offering has the business objects that support migration of HCM custom roles within its Users and Security functional area.

Before You Begin

Learn how to export and import business object data. Detailed instructions are available in the Overview of Setup Data Export and Import topic of the Using Functional Setup Manager guide. Refer to the Related Topics section for the link to this topic.

What Gets Exported and Imported

When you migrate HCM roles and security profiles, the following business objects are exported in the configuration package generated from the Users and Security functional area within the Workforce Deployment offering.

- Application Data Security
- Application Profile Value
- Functional Security Custom Roles
    - Functional Security Custom Role Hierarchy
    - Functional Security Custom Role Privilege Membership
- HCM Data Role
    - HCM Data Role Security Profile
- HCM Exclusion Role
    - HCM Exclusion Rule Detail
- Legislative Data Group Security Profile
    - Legislative Data Group Security Profile List
- Organization Security Profile
    - Organization Security Profile Classification List
    - Organization Security Profile Organization List
- Country Security Profile
    - Country Security Profile Country List
- Position Security Profile
    - Position Security Profile Position List
    - Position Security Profile Area of Responsibility Scope
- HR Document Type Security Profile List
    - HR Document Type Security Profile List
- Payroll Security Profile
    - Payroll Security Profile Pay
- Payroll Flow Security Profile
    - Payroll Flow Security Profile Pay

- Payroll Element Security Profile
  - Payroll Element Security Profile Details
- Person Security Profile
  - Person Security Profile Manager Type
  - Person Security Profile Area of Responsibility Scope
  - Person Security Profile Exclusion
- Talent Pools Security Profile
  - Talent Pools Security Profile Job Family
  - Talent Pools Security Profile Department
  - Talent Pools Security Profile Business Unit
- Transaction Security Profile
  - Transaction Security Profile Entries
  - Transaction Security Profile Sub Categories
- Role Provisioning Rule
  - Role Provisioning Associated Role List

Let's closely examine each business object to know what it contains.

Business Object	Information Included in Export and Import
Application Data Security	Application data security includes data security policies that are created in the following ways: • Manually using the Manage Database Resources page in the security console. • Manually using the Edit role/Copy role flow in the security console • Automatically when you copy a role using the Role Copy in the security profile • Automatically when you create profile content types • Automatically when you map HCM spreadsheet business objects to roles Data security policies that are generated by the HCM Data Roles UI aren't exported as part of the application data security business object. They're automatically created on the target environment when you import the HCM Data Role business object. Data security conditions that are generated from HCM security profiles aren't exported as part of the Application Data security business object. They're automatically created on the target environment when the HCM security profile business objects are imported. **Note:** There's no scope support for application data security policies. When you export application data security policies all data security policies are exported, even if you provided a scope value for other security business objects in your configuration package. There's no Export to CSV option for this business object.
Application Profile Value	Application profile value includes the profile values for the PER_MASTER_WORK_EMAIL profile.

Business Object	Information Included in Export and Import
	This profile option is no longer used and no values are exported for this business object.
Functional Security Custom Roles	The custom role includes the following details: - Role Code - Role Name - Role Description - Role Category - All IP Address Access - indicates that a role is granted access to the Security Control irrespective of the IP address from where it's signed in. **Note:** The scope is limited to User Assignable roles only.
Functional Security Custom Role Hierarchy	The role hierarchy includes the following details: - Parent Role - Member Role - Add or Remove Role Membership
Functional Security Custom Role Privilege Membership	The role privilege membership includes the following details: - Parent Role - Member Privilege - Add or Remove Privilege Membership
HCM Data Role	The HCM data role includes the following details: - Data Role Code - Data Role Name - Data Role Description - Inherited Job Role Code - Delegation Allowed Check Box
HCM Data Role Security Profile	The HCM data role security profile includes the following details: - Data Role Code - Securing Object - Security Profile Name
HCM Exclusion Rule	HCM exclusion rule and HCM exclusion rule detail includes HCM exclusion rule definitions. - HCM Exclusion Rule - HCM Exclusion Rule Detail
Legislative Data Group Security Profile List	Legislative data group security profile list includes the following details:

Business Object	Information Included in Export and Import
	• Legislative data group security profile name • Legislative data groups that are included in the legislative data group security profile
Organization Security Profile	Organization security profile includes the following details: • Organization Security Profile Name • Enabled Check Box • View All Check Box • Include Future Organizations Check Box • Code indicating Department Hierarchy or Generic Organization Hierarchy • Hierarchy Name (if securing by organization hierarchy) • Top Organization Name (if securing by organization hierarchy) • Include Top Organization Check Box • Secure by Organization Hierarchy Check Box • Secure by Organization Classification Check Box • Secure by Organization List Check Box
Organization Security Profile Classification List	Organization security profile classification list includes the following details: • Organization Security Profile Name • Organization Classification Name
Organization Security Profile Organization List	Organization security profile organization list includes the following details: • Organization Security Profile Name • Organization name • Organization Classification • Include/Exclude Check Box
Country Security Profile	Country security profile includes the following details: • Country Security Profile Name • Enabled Check Box
Country Security Profile List	Country security profile list includes the following details: • Country Security Profile Name • Country code
Position Security Profile	Position security profile includes the following details: • Position Security Profile Name • Description • Enabled Check Box • View All Check Box

Business Object	Information Included in Export and Import
	• Include Future Positions Check Box • Hierarchy Name (if securing by position hierarchy) • Top Position Name (if securing by position hierarchy) • Include Top Position Check Box • Top Position Name (if securing by organization hierarchy) • Secure by Position Hierarchy Check Box • Secure by Department Check Box • Department Organization Security Profile Name (if securing by department) • Secure by Business Unit Check Box • Business Unit Organization Security Profile Name (if securing by business unit) • Secure by Position List Check Box • Secure by Area of Responsibility Check Box
Position Security Profile Position List	Position security profile position list includes the following details: • Position Security Profile Name • Position Code • Include/Exclude Check Box
Position Security Profile Area of Responsibility Scope	Position security profile area of responsibility scope includes the following details: • Position Security Profile Name • Responsibility Type • Scope of Responsibility
HR Document Type Security Profile	HR document type security profile includes the following details: • HR Document Type Security Profile Name • Enabled Check Box • View All Check Box • Include/Exclude Check Box
HR Document Type Security Profile List	HR document type security profile list includes the following details: • HR Document Type Security Profile Name • Document Type Name
Payroll Security Profile	Payroll security profile includes the following details: • Payroll Security Profile Name • Enabled Check Box • View All Check Box
Payroll Security Profile Pay	Payroll security profile pay includes the following details: • Payroll Security Profile Name

Business Object	Information Included in Export and Import
	• Payroll Name • Legislative Data Group Name
Payroll Flow Security Profile	Payroll flow security profile includes the following details: • Payroll Flow Security Profile Name • Enabled Check Box • View All Check Box
Payroll Flow Security Profile Pay	Payroll flow security profile pay includes the following details: • Payroll Flow Security Profile Name • Flow Name
Payroll Element Security Profile	Payroll element security profile includes the following details: • Element Security Profile • Name
Payroll Element Security Profile Details	Payroll element security profile details includes the following details: • Name • Element Security Profile Details • Legislative Data Group Name • Classification Name • Element Name
Person Security Profile	Person security profile includes the following details: • Person Security Profile Name • Description • Enabled Check Box • Access to Own Record Check Box • Include Future People Check Box • Include Shared People Information Check Box • Access to Candidates with Offers Check Box • Secure by Area of Responsibility • Secure by Manager Hierarchy Check Box • Person or Assignment Check Box • Maximum Levels in Hierarchy • Manager Hierarchy Type • Hierarchy Content Code • Secure by Person Type Check Box • Secure by Department Check Box

Business Object	Information Included in Export and Import
	• Department Security Profile Name (if securing by department) • Secure by Business Unit Check Box • Business Unit Profile Name (if securing by business unit) • Secure by Legal Employer Check Box • Legal Employer Security Profile Name (if securing by legal employer) • Secure by Position Check Box • Position Security Profile Name (if securing by position) • Secure by Legislative Data Group Check Box • Legislative Data Group Security Profile Name (if securing by legislative group) • Secure by Payroll Check Box • Payroll Security Profile Name (if securing by payroll) • Secure by Global Name Range Check Box • Global Name Range Start Value (if securing by global name range) • Global Name Range End Value (if securing by global name range) • Apply Exclusion Rules Check Box • Secure by Custom Criteria Check Box • Custom Restriction Text (if securing by custom criteria) •
Person Security Profile Manager Type	Person security profile manager type includes the following details: • Person Security Profile Name • Manager Hierarchy Type (if something other than All or Line Manager has been selected on the security profile)
Person Security Profile Area of Responsibility Scope	Person security profile area of responsibility scope includes the following details: • Person Security Profile Name • Responsibility Type • Scope of Responsibility • Employee Check Box • Contingent Worker Check Box • Pending Worker Check Box • Nonworker Check Box • Candidate with Offer Check Box
Person Security Profile Exclusion	Person security profile exclusion includes the following details: • Person Security Profile Name • Exclusion Rule Name
Talent Pools Security Profile	Talent pools security profile includes the following details: • Talent Pool Security Profile Name

Business Object	Information Included in Export and Import
	- Enabled Check Box - View by Ownership Check Box - View All Check Box - View All Public Talent Pools Check Box - Secure by Business Unit Check Box - Secure by Department Check Box - Secure by Job Family Check Box
Talent Pools Security Profile Job Family	Talent pools security profile job family includes the following details: - Talent Pool Security Profile Name - Job Family Name
Talent Pools Security Profile Department	Talent pools security profile department includes the following details: - Talent Pool Security Profile Name - Department Name
Talent Pools Security Profile Business Unit	Talent pools security profile business unit includes the following details: - Talent Pool Security Profile Name - Business Unit Name
Transaction Security Profile	Transaction security profile includes the following details: - Transaction Security Profile Name - Description - Enabled Check Box - View All Check Box
Transaction Security Profile Entries	Transaction security profile entries include the following details: - Transaction Security Profile Name - Product Family - Category Code - All Sub Categories Check Box - Exclude Sub Category Check Box
Transaction Security Profile Sub Categories	Transaction security profile sub categories include the following details: - Transaction Security Profile Name - Product Family - Category Code - Sub Category Code
Role Provisioning Rule	Role provisioning rule includes the following details:

Business Object	Information Included in Export and Import
	- Mapping Rule Name - Legal Employer Name - Business Unit Name - Department Name - Job Set Code - Job Code - Position Business Unit Name - Position Code - Grade Set Code - Grade Code - Location Set Code - Location Code - User Person Type - System Person Type - Assignment Type - HR Assignment Status Code - Resource Role - Party Type Usage Code - Contact Role - Manager with Reports Check Box - Manager Type - Responsibility Type
Role Provisioning Associated Role List	Role provisioning associated role list includes the following details: - Mapping Rule Name - Role Code - Requestable Check Box - Self-Requestable Check Box - Autoprovision Check Box

Other business objects that you might like to export when migrating HCM custom roles are:

- Job Requisition Security Profile
- Spreadsheet Business Object Security Mapping

Let's closely examine each of these business objects to know what they contain.

Business Object	Information Included in Export and Import
Job Requisition Security Profile	Job requisition security profile includes the following details:

Business Object	Information Included in Export and Import
	• Job Requisition Security Profile Name • Enabled Check Box • View All Check Box • Secure by Job Family Check Box • Secure by Job Function Check Box • Secure by Location Check Box • Secure by Organization Check Box • Secure by Recruiting Type Check Box
Spreadsheet Business Object Security Mapping	HCM spreadsheet business object access mapping includes the following details: • Role Code • Business Object • Product Area • Enabled Check Box • All Business Objects Check Box

You can migrate job requisition security profiles by exporting the business objects in the Users and Security functional area within the Recruiting and Candidate Experience offering. You should do this before migrating the business objects in the Users and Security functional area within the Workforce Deployment offering. You must have the Recruiting Administrator role to export and import job requisition security profiles.

You can migrate HCM spreadsheet business object access mappings by exporting the business objects in the HCM Data Loader functional area within the Workforce Deployment offering. You should do this after migrating the business objects in the Users and Security functional area. You must have the Human Capital Management Integration Specialist role to export and import HCM spreadsheet business object access mappings.

After the Import Completes

You might need to wait for a period of time before all of the migrated data security policies are visible in the security console after completing the import of the configuration package that's generated from the Users and Security functional area within the Workforce Deployment.

When application data security policies are imported, a process runs in the background to synchronize the imported data security policies with the roles on the target environment. The imported data security policies aren't active until this process has completed, at which point the data security policies will be visible in the security console. This affects data security policies for custom roles that have been copied from other roles in the source environment. It also affects custom roles that have data security policies that were added manually using the security console.

> **Note:** No manual regeneration processes are needed on the target environment; the import process triggers the role regeneration process. This only applies if you're importing the HCM Data Role business object.

What's Not Included

Data security policies that have been manually created from the security console, and which reference conditions that have been generated from an HCM security profile, must be manually recreated on the target environment. You must import the condition by importing the appropriate HCM security profile business object before creating these data security policies in the target environment.

Related Topics

- Overview of Setup Data Export and Import

Export and Import a Custom Role

You can export and import a custom role that has data security policies using an implementation project. The tasks in your implementation project and their sequence determine the list of setup business objects whose data is exported and imported, and in which order.

This method is useful if you want to export and import one or more custom job or abstract roles without security profiles.

Create an Implementation Project

Follow the steps below to create an implementation project.

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. In the Setup page, select **Manage Implementation Projects** from the **Tasks** panel tab.
3. In the Manage Implementation Projects page, select **Create** from the **Actions** menu, or click the **Create** icon.
4. In the Create Implementation Project: Basic Information page, enter a meaningful name and a brief description to describe your project.
5. Click **Save and Open Project**.

   A page with the name you specified for your implementation project opens. The task list is empty.
6. Select **Create** from the **Actions** menu, or click the **Create** icon and add the following tasks to your implementation project:

   - Manage Job Roles
   - Manage Data Security Policies
7. Click **Done**.

Export Role Definitions Using an Implementation Project

Follow the steps below to export your custom role definitions using your implementation project.

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. In the Setup page, select **Manage Configuration Packages** from the Tasks panel tab.
3. In the Manage Implementation Projects page, select **Create** from the **Actions** menu, or click the **Create** icon from the Search Results table in the Manage Configuration Packages page to go to the Create Configuration Package: Enter Basic Information page.
4. Select the implementation project you created earlier from the **Name** menu.

   a. If you see a message warning you that the implementation project doesn't contain any offering, click **Yes** to continue.
   b. Leave the default selection for **Export**, **Setup task list and setup data** unchanged.

5. In Configuration Package Details, you can use the default field values for **Name, Code** and **Description**, or assign unique values.
6. Click **Next** to go to the Create Configuration Packages: Select Objects for Export page.

   The first table displays the list of business objects whose setup data is exported:

   - Application Data Security Policy
   - Functional Security Custom Roles
   - Functional Security Custom Role Hierarchy
   - Functional Security Custom Role Privilege Membership

     All of the business objects have their **Export** column checked by default. Keep this selection unchanged.

     It's best if the Application Data Security business object is imported after the other three business objects. Change the import sequence for the Application Data Security Policy business object so that it has a higher value than the import sequence for the other business objects.
7. Select the custom roles that you want to export.

   a. Select the Functional Security Custom Roles business object in the first table.
   b. Click the **Create** icon in the scope table.
   c. Search and select the custom role you ant to export and click **Apply.** If you want to export more than one custom role, repeat this step for each role you want to export.
   d. Click **Save and Close** when you have finished selecting all the roles you want to export.

> **Note:** There is no scope support for data security policies. Refer to the *What Gets Exported and Imported* section of the *Export and Import of HCM Custom Roles and Security Profiles* topic for detailed information on which data security policies will be exported.

8. Click **Submit** to submit the setup data export process and **Confirm** when the confirmation message appears.
9. Monitor the process from **Manage Configuration Package** until it completes.
10. While the process is in progress, you may select the status to go to the Export and Import Process Results page to view how much progress the process has made at the time. Click the **Refresh** button to get the most recent information. Refer to the Review of Export and Import Process Results topic for detailed descriptions of the process results.
11. Once the export process completes successfully, click **Download** to download the configuration package. Use this .zip file to import setup data in the target environment. Optionally, select the status to go to the Export and Import Process Results page to view the result details.

Import Role Definitions Using an Implementation Project

Follow these steps in the Import Setup Data Using Implementation Project topic of the Using Functional Setup Manager guide. Refer to the Related Topics section below for the link to this topic.

Related Topics

- Manage Setup Using Implementation Projects
- Export Setup Data Using Implementation Project
- Import Setup Data Using Implementation Project

11 Preparing for Application Users

Overview of Preparing for HCM Application Users

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 for each user category on the Security Console before creating application users.

Related Topics

- User and Role-Provisioning Setup Options
- Set the User and Role Provisioning Options
- User-Name Formats
- Password Policy
- User-Name and Password Notifications

User and Role-Provisioning Setup Options

User and role-provisioning options control the default management of some user-account features. To set these options, perform the Manage Enterprise HCM Information task in the Workforce Structures functional area for your offering. You can edit these values and specify an effective start date.

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

> **Note:** User accounts without roles are suspended automatically. Therefore, roles are provisioned automatically at account creation to avoid this automatic suspension.

The **User Account Creation** 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

After 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.

Related Topics

- User Account Creation Option
- User Account Role Provisioning Option
- User Account Maintenance Option
- User Account Creation for Terminated Workers Option

User Account Creation Option

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

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.

> **Note:** When a user account is created, roles may be provisioned to it automatically based on current role-provisioning rules. This provisioning occurs because user accounts without roles are suspended automatically. Automatic creation of user accounts and the associated role provisioning are controlled by the **User Account Creation** option.

User Account Maintenance Option

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.

Value	Description
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

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.

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

- Why You Should Run the Send Pending LDAP Requests Process

Set the User and Role Provisioning Options

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.

1. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Workforce Structures
    - Task: Manage Enterprise HCM Information
2. On the Enterprise page, select **Edit** > **Update**.
3. In the Update Enterprise dialog box, enter the effective date of any changes and click **OK**. The Edit Enterprise page opens.
4. Scroll down to the User and Role Provisioning Information section.
5. 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**.
6. Click **Submit** to save your changes.
7. Click **OK** to close the Confirmation dialog box.

Related Topics

- User and Role-Provisioning Setup Options

Provision Abstract Roles to Users Automatically

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.

Provision the Employee Role Automatically to Employees

1. Sign in as the TechAdmin user or another user with the IT Security Manager (ORA_FND_IT_SECURITY_MANAGER_JOB) job role or privileges.
2. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Users and Security
    - Task: Manage Role Provisioning Rules

3. In the Search Results section of the **Manage Role Mappings** page, click the **Create** icon. The **Create Role Mapping** page opens.
4. In the **Mapping Name** field, enter **Employee**.
5. 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

6. In the Associated Roles section of the **Create Role Mapping** page, add a row.
7. In the **Role Name** field of the Associated Roles section, click **Search**.
8. In the Search and Select dialog box, enter **Employee** in the **Role Name** field and click **Search**.
9. Select **Employee** in the search results and click **OK**.
10. If **Autoprovision** isn't selected automatically, then select it. Ensure that the **Requestable** and **Self-Requestable** options aren't selected.
11. Click **Save and Close**.

Provision 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 4, enter **Contingent Worker** as the mapping name.
- In step 5, set **System Person Type** to **Contingent Worker**.
- In steps 8 and 9, search for and select the Contingent Worker role.

Provision the Line Manager Role Automatically to Line Managers

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
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 Fusion Cloud Human Capital Management.

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 (Doc ID 2004494.1)

12 Creating Application Users

Options for Creating HCM Application Users

When you create person records in Oracle HCM Cloud, user accounts can be created automatically. The User and Role Provisioning options control whether user accounts are created and maintained automatically. You set these options for enterprise 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 with basic person records 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**. If you're creating user accounts for uploaded workers, then you can provide a user name in the uploaded data. This value overrides the default user-name format for the default user category. 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.

Related Topics

- Create Oracle HCM Cloud Users Using the New Person Tasks
- Create Oracle HCM Cloud Users Using the Create User Task
- Provision Abstract Roles to Users Automatically

Create Oracle HCM Cloud Users Using the New Person Tasks

Once the initial implementation of Oracle HCM Cloud is complete, you can create person records.

You can create the person records in either of the following ways:

- 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.

Hire an Employee: User-Name Values

You must have the Human Resource Specialist job role to hire an employee as described here. Follow these steps:

1. 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**.

   > **Tip:** New users belong to the default user category. Therefore, the default user-name format is the format defined for the default user category. You can add the user to a different user category after the user account exists.

4. You enter the person's first and last names. Other names are optional. The user name is based on the person's first and last names if the generation rule for user names in the default user category 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 email. If you enter no work email when you create the person record, then an authorized user can enter it later on the Security Console. You can't add it directly to the person record later. After the person record exists, the email is managed on the Security Console.

   The user name is the work email if the generation rule for user names in the default user category is **Email**.
7. Click **Next**.

Hire 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

   > **Note:** User-account and role-provisioning requests are processed only if processing is enabled for the enterprise.

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

Create Oracle HCM Cloud Users Using the Create User Task

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 after 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** > **Users and Roles** to open the Search Person page.
2. In the Search Results section, click the **Create** icon.

   The Create User page opens.

Enter Personal Details

Follow these steps:

1. Enter the user's name.
2. In the **Email** field, enter the user's primary work email.

   > **Tip:** If email validation is enabled, then a warning appears if the email already exists.
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 after the user exists.

Enter User Details

You can either create a user account or link an existing, standalone user account.

To create a user account, you select **Enter user name**. If you leave the **User Name** field blank, then the user name is generated automatically in the enterprise default format. In this case, automatic creation of user accounts must be enabled for the enterprise. If you enter a user name, then that name is used if valid.

Alternatively, you might have created a standalone user account on the Security Console or using SCIM (REST) APIs. These types of user accounts aren't linked to person records. To link such an account to the new person record:

1. Select **Link user account**.
2. Click the **Link** icon to open the Link User Account dialog box.
3. In the Link User Account dialog box, search for and select the user account. Accounts that are already linked to person records don't appear here. The account can be in any status. Its status isn't changed when you link it.
4. Click **OK** to link the account.

> **Tip:** On the Edit User page, you can edit the user details and link a different user account, if required. The link to the existing user account is removed automatically.

Set 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 for the default user category on the Security Console.
- An appropriate notification template exists.

For example, if the predefined New Account Template notification template is enabled for the default user category, then a notification is sent to the user.

If you deselect this option, then you can send the notification later by running the **Send User Name and Password Email Notifications** process. The notification is sent to the user's work email. If the user has no work email, then the notification is sent to the user's line manager. Appropriate notification templates must be enabled at that time.

Enter Employment Information

Follow these steps:

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

Add Roles

Follow these steps:

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.

   > **Note:** If you linked an existing user account, then any roles that were already assigned externally and manually to the account appear in the Roles section. When you click **Autoprovision Roles**, the user's entitlement to those roles is reviewed. If the user doesn't qualify for the roles, based on the employment information entered so far, then their removal is requested.

2. To provision a role manually to the user, click the **Add Role** icon. 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**.

Related Topics

- Enable Validation of Work Email for Users and Roles

Enable Validation of Work Email for Users and Roles

You can enable validation of the email that you enter on the Create User and Edit User pages. When validation is enabled, a warning message appears if you enter a duplicate value.

The message provides the name, the user name, or both of the email owner. Having this warning enables you to enter a unique email before saving. Validation of the email on the **Create User** and **Edit User** pages is disabled by default. This topic explains how to enable validation of the email value on these pages.

Enable Email Validation

To enable validation, you set the profile option, PER_MANAGE_USERS_EMAIL_VALIDATION.

To set the profile option, follow these steps:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, enter **PER_MANAGE_USERS_EMAIL_VALIDATION** in the **Profile Option Code** field and click **Search**.
3. In the Profile Values section of the search results, enter **Y** in the **Profile Value** field.
4. Click **Save and Close**.

> **Note:** When validation of the work email is enabled, it applies to the Create User and Edit User pages. It doesn't apply to user accounts that you manage on the Security Console.

FAQs for Creating Application Users

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

When you create a person record, a user account is created automatically 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 or using SCIM (REST) APIs.

You can link the account to the person record using the Manage User Account or Create User 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 for the user category. The default format is the worker's primary work email, but you can override this value for each user category.

For example, your enterprise may use person number as the default user name for the default user category.

13 Managing Application Users

Manage HCM User Accounts

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

To access the user account page for a person:

1. On the **My Client Groups** tab, find and select the **Manage User Account** quick action. You must click **Show More** if it isn't visible by default.
2. Search for and select the person whose account you're updating.

IT Security Managers can manage user accounts and user roles using the security console. For more information, see the topic *Oracle Fusion Applications Security Console* .

Manage 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. The list of available roles is decided by role provisioning rules that have been configured using the Role Mappings UI.
3. In the search results, select the role and click **OK**.
4. Click **Save**.

To remove a role:

1. Select the role and click **Remove**.
2. In the Warning dialog box, click **Yes** to continue.
3. Click **Save**.

To update a user's roles automatically, select **Actions** > **Update Role Assignments**. 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 they qualify but don't currently have
- Loses any role for which they no longer qualify

You're recommended to autoprovision roles for individual users if you know that additional or updated role mappings exist that affect those users.

Synchronize Personal Data with Identity Store

By default, changes to personal data, such as person name and phone, are copied to your Identity Store periodically. To copy any changes immediately:

1. Select **Actions** > **Synchronize with Identity Store**.
2. Click **Synchronize**.

Reset 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 email.
   > **Note:** A notification template for the password-reset event must exist and be enabled for the user's user category. Otherwise, no notification is sent.

Edit 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 Identity Store. 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.

User Names

By default, user names are generated automatically in the format specified for the default user category when you create a person record. Users who have the human resource specialist (HR specialist) role can change user names for existing HCM users.

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 format specified for the default user category. This table summarizes the effects of the available formats for Oracle Fusion Cloud HCM users.

User-Name Format	Description
Email	The worker's work email is the user name. If you don't enter the work email 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 Security Console.
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.

User-Name Format	Description
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 you can disable it 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. On the **My Client Groups** tab, find and select the **Manage User Account** quick action. You may have to click **Show More** if it is not visible by default. Line Managers can use the quick action on the My Team tab.
2. Search for and select the worker.
3. On the Manage User Account page, select **Actions** > **Edit User Name**.
4. Select **Actions** >

The updated name, which can be in any format, is sent automatically to your Identity Store. 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.

Why You Send Personal Data to Identity Store

User accounts for users of Oracle Fusion Applications are maintained on your Identity Store. By default, Oracle Fusion Cloud HCM sends some personal information about users to the Identity Store.

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 Identity Store.

Bulk Creation of Users

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

When you load person records in bulk, the order in which they're created 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 Identity Store 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 Identity Store 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 Identity Store, 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 Identity Store (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.

Synchronize Personal Data with the Identity Store

Users can synchronize their personal data with the Identity Store 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 Identity Store directory. However, this action is available for copying changes immediately, if necessary.

Related Topics

- User and Role-Provisioning Setup Options

How You Manage an Incomplete Request for an HCM User Account

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 email 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.

Link an Existing User Account to a Person Record

By default, when you create person records, user accounts are created automatically in your Identity Store and linked to those person records. However, this automatic creation of user accounts can be disabled for the enterprise.

For example, you might have some other way of managing user accounts, or user accounts might already exist in your Identity Store. In this case, you must link the existing 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 have access to the person record to perform this task.

Follow these steps:

1. On the **My Client Groups** tab, find and select the **Manage User Account** quick action. You might have to click Show More if it is not visible by default.
2. Search for and select the worker.
3. On the **Manage User Account** page, if the person you have selected has no user account, then you're prompted to select one of the following two actions:
    - Create a User Account
    - Link an Existing User Account
4. Click **Link an Existing User Account**.
5. On the **Link User Account** page, search for and select the user name from the drop-down list.

   The list contains only those user accounts that aren't already linked to an Oracle HCM Cloud person record.
6. Click **Save and Close** to close the Link User Account dialog box.

Any roles that were already assigned externally and manually to the linked user account appear in the Current Roles section. If the user doesn't qualify for those roles, based on current employment information, then their removal is requested. 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**.

You can also link an existing user account to a person record on the Create User and Edit User pages.

How User Accounts Are Suspended

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** > **Users and Roles**.
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 are updated only when 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

How You Manage Application Users on the Security Console

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 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.
- Provision roles to implementation users.
- Reset user passwords, provided that the **Administrator can manually reset password** option is selected for the relevant user category.

On the User Categories page of the Security Console, IT Security Managers can create and manage user categories. For any category, they can:

- Define the default format of user names.
- Set the password policy.
- Manage notifications.
- Add users to and remove users from the category.

Create a Custom Role with Limited Access

To delegate some of the IT security management tasks to a helpdesk member within your company without assigning the IT Security Manager role, create a custom role with specific privileges.

These privileges are exclusively meant for controlling user management access. You can assign these privileges directly to a custom role.

Users without the IT Security Manager role who are assigned custom roles with these privileges have limited access to the Security Console. These users can only lock or unlock other users, reset their password, or view user details. They can't create users or edit user details.

The following table lists the privileges and the associated access controls. It also includes details of pages where the user does the task:

Table with Privileges, Access Control Details, and Pages Where User Does the Task

Privilege Name and Code	Access Control Details	Page Where You Do this Task
Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)	Lock or unlock a user account	User Accounts
Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)	Reset the password for a user account	User Accounts and User Account Details
View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)	View the details of a user account	User Account Details

Related Topics

- View Locked Users and Unlock Users
- Reset Passwords

Get User Sign-in Sign-out Information

You can get the last seven days of user sign-in sign-out information using a setting available on the Add User Account page in Security Console. To view the setting, you must enable a profile option.

You can access the sign-in sign-out information through REST APIs. For more information, see the topic Sign In and Sign Out Audit REST Endpoints in *REST API for Common Features in Oracle Fusion Cloud Applications* on the Oracle Help Center.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**: ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the **Profile Value** drop-down list, select **Yes**.
4. Click Save and Close.

> **Note:** The audit data is available for seven days.

The profile option is enabled. On the Add User Account page in Security Console, the setting to get user sign-in sign-out information appears now in the Advanced Information section.

On the Security Console, click **Users**. On the User Accounts page, click **Add User Account** and select **Enable Administration Access for Sign In-Sign Out Audit REST API**. You can also enable this option on the User Account Details Edit page.

Provide Read-Only Access

Some users may need read-only access to Oracle HCM Cloud. The Read Only Mode (FND_READ_ONLY_MODE) profile option controls read-only access.

This topic describes how to set Read Only Mode for specific users. Some situations in which read-only access is required are:

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

Set the Read Only Mode Profile Option

To enable read-only mode for a user:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. 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**.
3. In the FND_READ_ONLY_MODE: Profile Values section of the page, click the **New** icon.
4. 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.
5. 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 assign to a user?

You can see the roles that you want to assign, if the role satisfies all of the following conditions:

- A role mapping exists for the role. For more information on creating a role mapping, see the topic *Create a Role Mapping*.

- The Requestable option is selected for the role in the role mapping. For more information, see the topic *How do I provision HCM data roles to users?*.
- At least one of your assignments satisfies the role-mapping conditions.

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 such an account to the worker's person record on the **Manage User Account**, **Create User**, or **Edit User** page.

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 Identity Store?

User accounts are defined in your Identity Store. The Identity Store also holds some personal information about users, such as name, work phone, and work location address. Changes to personal information in Oracle HCM Cloud are copied automatically at intervals to your Identity Store.

What happens if I send the user name and password?

The user name and password go to the work email 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 **Send User Name and Password Email Notifications** process.

What happens if I reset a user's password?

A notification containing a reset-password link is sent to the user's work email. If the user has no work email, then the notification is sent to the user's line manager. Notification templates for this event must exist and be enabled.

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

You can run the Send User Name and Password Email Notifications process in the Scheduled Processes work area. For users for whom you haven't so far requested an email, this process sends out user names and reset-password links.

The email goes to the work email 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?

Yes, but be careful how you use it. User impersonation (Set Preferences Proxies) allows a proxy user to do tasks on your behalf in an impersonation session. The proxy user has the same access to your data as you do.

The proxy user acquires all of your roles, which is unsafe if you use employee self-service. As an HCM Cloud user, remember that your proxies will have access to your personal and sensitive information, such as your salary details, national IDs, and so on.

14 Provisioning Roles to Application Users

Role Mappings

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** task in the Setup and Maintenance work area to provision roles.

> **Note:** 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 conditions shown in this table.

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 conditions shown in this table.

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 conditions shown in this table.

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.

Related Topics

- Examples of Role Mappings
- Autoprovisioning

Create a Role Mapping

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. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Manage Role Provisioning Rules
2. In the Search Results section of the Manage Role Mappings page, click **Create**.

   The Create Role Mapping page opens.

Define the Role-Mapping Conditions

Set values in the Conditions section to specify when the role mapping applies. For example, the values shown in this table limit the 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.

Identify the Roles

1. In the Associated Roles section, click **Add Row**.
2. In the **Role Name** field, search for and select the role that you're provisioning. For example, search for the data role **Procurement Analyst Denver**.

3. Select one or more of the role-provisioning options shown in this table.

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

Apply 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 autoprovisioning requests.

Related Topics

- Autoprovisioning

Examples of Role Mappings

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 conditions shown in this table.

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 conditions shown in this table.

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 conditions shown in this table.

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

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 Fusion Cloud HCM 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

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.

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. These requests are processed by the **Send Pending LDAP Requests** process. When running **Autoprovision Roles for All Users**, 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 the process can run at a time.

Options for the Process

When processing a large number of requests, you can enable bulk mode for this process to improve performance. In the bulk mode, the process groups all users for the same role into one request, and assigns multiple users to single role at once. In the default non-bulk mode, one user is assigned to a role at a time.

To enable bulk mode, follow these steps:

1. In the Setup and Maintenance work area, search and open the task **Manage Profile Options**.
2. In the **Search Results** section, click the + (New) icon.
3. On the **Create Profile Option** page, enter the following values:
   - Profile Option Code = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
   - Profile Display Name = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
   - Application = Global Human Resources
   - Module = Users
   - Start Date = <Today's date>

   Click **Save and Close**.
4. On the **Manage Profile Options** page, select the **Enabled** and **Updateable** check boxes for Site Level. Click Save and Close.
5. In the Setup and Maintenance work area, search and open the **Manage Administrator Profile Values** task.

6. Search for the profile option code PER_AUTO_PROVISION_ROLES_ENABLE_BULK. In the Profile Value text box, enter 'Y'. Note that this value is for one-time use, and you need to reset the value again for the next run of the process. Click **Save and Close**.

You can enable multithreading for the process by setting the profile option ORA_PER_AUTO_PROVISION_ROLES_ENABLE_MULTITHREADING to 'Y'. This creates child jobs, which help in improving the performance.

For more information, see the topic Best Practices for User and Role Provisioning in HCM.

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?
- Schedule the Send Pending LDAP Requests Process
- Best Practices for User and Role Provisioning in HCM

Guidelines for Editing Role Mappings

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. You should also run this process after loading person records in bulk if no role mapping exists for those person records before the load.

- A human resource (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.

Related Topics

- Role Provisioning and Deprovisioning
- Autoprovisioning

Best Practices for User and Role Provisioning in HCM

These best practices and guidelines help you to identify the processes used for user and role provisioning in HCM. We'll present different examples and scenarios to explain how these processes should be used.

Understanding the proper execution of these processes helps support stability and manage resources responsibly.

User and Role Provisioning Processes

There are four processes for user and role provisioning. You should run only one of these processes at a time. These processes should never overlap. Make sure you allow time for one process to complete before scheduling another process.

Here are the four user and role provisioning processes:

Process	Purpose	How Often	Usage	Best Practices
Send Pending LDAP Requests	Sends to the LDAP directory the requests related to user account	Daily As needed	This job processes requests to:	DOs

Process	Purpose	How Often	Usage	Best Practices
	provisioning as well as the requests for adding and removing user roles. You typically use this to process the provisioning requests created by bulk processes as well as to process future dated requests that are now active.		• Create, suspend, and reactivate user accounts • Provision and deprovision roles • Update person attributes for individual users including work emails • Send information about HCM data roles which originate in Oracle HCM Cloud Parameters usage: • **`User Type`** ○ All - Process requests for all user types. Recommended. ○ Party - Process requests only for CRM parties. ○ Person - Process requests only for HCM persons. • **`Batch Size`** - Number of batches to process the pending requests ○ A - Uses batch size of 10. Recommended. ○ AF - Uses batch size of 10, but each run also processes requests that failed in previous runs. ○ 20 - Used only when processing very large number of requests. For more information, see the topic *Why You Should Run the Send Pending LDAP Requests Process*.	• Schedule at least once a day with Batch Size as A. • If required, schedule to run more than once a day based on your requirement. Make sure the next run starts at least 30 minutes after the completion of previous run. • Run the job after loading workers or users in bulk using HCM Data Loader. For more information, see the topic *Processes to Run After Loading Data* from the HCM Data Loader guide. DON'Ts • Don't schedule to run in intervals of less than 30 minutes. Running the job too frequently can result in unnecessary processing overhead for the application and can result in performance issues. • Don't schedule to run with Batch Size as AF. ○ Batch Size AF should only be used to run the job manually to reprocess faulted requests after issues are resolved. ○ If scheduled to run with Batch Size AF, each time the job runs, it creates new LDAP requests for faulted requests to reprocess them. If the underlying issue for the fault is not resolved, it will keep creating new LDAP requests over and over again. • Don't schedule to run with Batch Size > 20. Default batch size is 10 (A) and recommended

Process	Purpose	How Often	Usage	Best Practices
				maximum batch size is 20.
Auto provision Roles for All Users	Evaluates roles membership for all users, including inactive users, against the role provisioning rules.	As needed Rarely	This process compares all current user assignments with all current role mappings and creates required requests to add or remove roles to users. Parameters Usage • **`Process Generated Role Requests`** - Indicates whether the job should process the generated LDAP requests ○ Yes - When the number of role requests generated is expected to be small, set the parameter to Yes so this job also processes the generated requests. ○ No - When thousands of role requests are expected to be generated, set the parameter to No, to defer the processing to next run of Send Pending LDAP Requests job. • **`Worker Assignment Status`** - Assignment status of workers for whom the autoprovisioning rules should be performed by the job ○ Active ○ Active, Suspended ○ Inactive ○ Suspended To improve performance while processing large number of requests, enable Bulk Mode for this job.	DOs Run the job once on demand for below scenarios: • Initial role assignment for existing users after creating role mappings • When new role-mapping rules are added or existing rules changed For more information, see the topic *Autoprovisioning*. DON'Ts • Don't schedule to run regularly since this job evaluates all the role-mapping rules and validates them for the entire user population, which is a costly operation. ○ After initial role assignments are done, role-mapping rules are performed incrementally every time workers are created/updated/ terminated ○ More the number of role-mapping rules and number of users, the longer and costlier are the processing done by this job • Running the job too frequently can result in unnecessary processing overhead for the application and can result in performance issues.
Send Personal Data for Multiple Users to LDAP	Reconciles personal information changes in Oracle HCM Cloud with LDAP directory.	As needed Rarely	For HCM person records updated in bulk, this process updates their personal data in LDAP to match with their data in Oracle HCM Cloud. This process updates First	DOs • Run once on demand with parameter **`All Users`** only as one-time synchronization of all user records to

Process	Purpose	How Often	Usage	Best Practices
			Name, Last Name, Email, and Manager attributes. This process applies only to HCM person users and not to party users. Parameters Usage • **`User Population`** ○ All users ○ Changed users only For more information, see the topic *Why You Send Personal Data to Identity Store*.	LDAP during initial implementation. • Run once on demand with parameter **`Changed users only`** after changing personal data of workers in bulk. The job then synchronizes personal data only for those changed users to LDAP. For more information, see the topic *Processes to Run After Loading Data*. DON'Ts • Don't schedule to run regularly with parameter **`All Users`**, since each time the job is run, it creates an LDAP request for each user regardless of whether personal information was changed or not. If the job is scheduled, it creates two issues: ○ Create unnecessary LDAP requests for all users in the application causing the LDAP requests table to grow in size. ○ Cause unnecessary processing overhead for **Send Pending LDAP Requests** job and can result in performance issues.
Retrieve Latest LDAP Changes	Updates the Oracle HCM Cloud person records with data coming from the LDAP directory.	Very rarely	This process synchronizes all users and roles from LDAP directory to Oracle HCM Cloud. If a difference is noticed between roles provisioned to a user in **Security Console** and roles on the **Manage User Account** page, it is recommended to run this process. This job does not have any parameters. For more information, see the topic *Retrieve Latest LDAP Changes*.	DOs Run once on demand in below scenarios: • After a release update • User/role records in Oracle HCM Cloud are out-of-synch with LDAP and confirmed by Oracle Support to run the job **DON'Ts** • Don't schedule to run regularly since it is unnecessary

Process	Purpose	How Often	Usage	Best Practices
				processing and does not serve any functional purpose. All the user data are first created in Oracle HCM Cloud and synchronized to LDAP. User records aren't expected to be changed directly in LDAP so there is no requirement to retrieve changes regularly from LDAP to Oracle HCM Cloud.

Common Scenarios of User and Role Provisioning Processes

Let's go through several scenarios to better understand the user and role provisioning processes. Some of the processes have the potential to slow down your environment, so we recommend familiarizing yourself with these scenarios to understand the impact before scheduling a process.

Scenario 1: Importing New Hires Using HCM Data Loader

- The User Account Creation option on the Manage HCM Enterprise Information page is set to Both person and party users. This setting ensures that the user account is automatically generated when each worker is imported.
- New Hires are loaded by using HCM Data Loader to import the Worker.dat file.
- User Account requests are created automatically for each imported person.

What you should do next:

After completing the import of New Hires using HCM Data Loader, run the **Send Pending LDAP Requests** process once. This job sends all pending user account create requests from the HCM Cloud to the LDAP directory.

What you should not do:

- Auto provision Roles for All Users
- Retrieve Latest LDAP Changes
- Copy Personal Data for All Users to LDAP

Scenario 2: Changes in Manage Role Provisioning Rules in your Organization

Your organization is making changes to Manage Role Provisioning Rules by adding new role provisioning rules, or by updating existing role provisioning rules. These changes may impact how the roles should be assigned to new or existing users.

What you should do next:

After the update of auto provisioning mapping is completed:

- Run the Auto provision Roles for All Users process once with default parameters.

This job will evaluate every user, including active and inactive users, and will update role memberships according to updated role auto provisioning rules. This is the only situation when you should run this process in a production environment.

Scenario 3: Workers were Imported Before Auto provisioning Mappings in Manage Role Provisioning Rules Were Created

Your organization imported workers and created user accounts for them without first creating role provisioning rules using the Manage Role Provisioning Rules task. Existing user accounts were not evaluated against new role provisioning rules.

What you should do next:

It's critical to avoid this situation. All role-provisioning rules should be created before the workers are loaded in bulk, at a minimum the Employee role rule must be created.

After the roles provisioning rules are created, run:

- The Auto provision Roles for All Users process once with default parameters. This job evaluates, including active and inactive users, and will update role memberships according to updated role auto provisioning rules.

Scenario 4: Manual Update of Employee's Manager, First Name, Last Name, or Email

You have a short list of employees and you're going to use the application to update one of the following fields:

- First Name
- Last Name
- Email
- Manager

What you should do next:

Nothing. This HR transaction doesn't require any user provisioning related activities.

What you should not do:

Don't run or schedule any of the user and role provisioning processes after this HR transaction completes.

Scenario 5: Bulk update of Employee's Manager, First Name, Last Name, or Email

You're going to update the following employee (worker) fields in bulk using HCM Data Loader:

- First Name
- Last Name
- Email
- Manager

And, you're not sure if this change requires additional user-related activities.

What you should do next:

After importing the updated worker information using HCM Data Loader:

- Run the Send Personal Data for Multiple Users to LDAP once.

  This job will update the LDAP records with person profile changes completed by the HCM Data Loader import. Be sure to run the job in Changed mode, not All Users mode.
- Run the Send Pending LDAP Requests process only when email was updated. This keeps the LDAP directory in sync.

Scenario 6: Manual Update of Employee's Assignment Location

You have an employee who changed job locations. You're going to update their assignment location using the application interface. Changing the employee's location may affect their role assignment.

What you should do next:

Nothing. This HR transaction automatically evaluates this employee against the role auto provisioning rules. If any changes are required in this employee's role memberships, they will be automatically completed when you save your HR transaction.

What you should not do:

Don't run or schedule any of the user and role provisioning processes after this HR transaction completes.

Scenario 7: You manually added job roles to a person

You were asked to add job roles to the selected employee manually and you're not sure if there's anything else to do with the LDAP directory.

What you should do next:

Nothing. This HR transaction automatically processes pending LDAP requests for the selected employee.

What you should not do:

Don't run or schedule any of the user and role provisioning processes after this HR transaction completes.

Scenario 8: Workers were loaded with HCM Data Loader with suppressed user account creation

Workers were loaded with suppressed user account creation, Counter-intelligences = N, and you're not sure if there's anything else you need to do with the LDAP directory.

What you should do next:

Nothing. Imported workers aren't expected to have user accounts so there's no need to run any additional LAP-related processes.

What you should not do:

Don't run or schedule any of the user and role provisioning processes after this HR transaction completes.

Scenario 9: User accounts were created for existing person records using HCM Data Loader

Workers were loaded without creating user accounts. You're going to create user accounts for existing workers in bulk by using HCM Data Loader to import the properly prepared User.dat file. You're also assigning some manual roles to new user accounts using this same method.

You're concerned about auto provisioning roles and don't know if there's anything else to do with LDAP processes.

What you should do next:

- After completing the import of the User.dat file using HCM Data Loader, run the Send Pending LDAP Requests once.

  This job sends all pending user account and role assignment requests from HCM to the LDAP directory. Every new user account will also be evaluated against the auto provisioning rules during the creation process.

What you should not do:

After loading user account requests with HCM Data Loader, don't schedule any of the following processes:

- Auto provision Roles for All Users
- Retrieve Latest LDAP Changes
- Copy Personal Data for All Users to LDAP

Scenario 10: You need to run the Auto provision Roles for All Users process and have a large volume of user accounts

You want to run the process initially for employees with active assignments ahead of other assignment status. The **Auto provision Roles for All Users** process picks up all user accounts every time it runs. This might have a long runtime when there is a large volume of user accounts. You can overcome this using an optional filtering parameter, **`Employee's Assignment Status`**.

The **`Employee's Assignment Status`** parameter lets you process only those user accounts linked to workers, whose assignment is in the selected status. It can have one of the following values:

- [Blank] - Default
- Active
- Active, Suspended
- Inactive
- Suspended

What you should do next:

After the update of auto provisioning is completed for the specific assignment status, run the **Auto provision Roles for All Users** process once with the default parameters. This job evaluates every user, including active and inactive users, and will update role memberships according to updated role auto provisioning rules. This is the only situation when you should run this process in a production environment.

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.

Can I use descriptive flexfields in role mappings?

Yes, you can model the role mapping based on non typical criteria using the custom assignment descriptive flexfields.

These custom assignment attributes are hidden by default, but can be displayed by enabling the predefined profile option **ORA_PER_ROLE_MAPPINGS_UI_DISPLAY_CUSTOM_ATTRIBUTES**. Only global segments can be used in role mappings.

To enable this profile option:

1. In the **Setup and Maintenance** work area, search for and select the task **Manage Administrator Profile Values**.
2. On the **Manage Administrator Profile Values page**, search for the profile option code **ORA_PER_ROLE_MAPPINGS_UI_DISPLAY_CUSTOM_ATTRIBUTES**.
3. Set the profile value to Y.
4. Click **Save and Close**.

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.

Provisioning Method	Meaning
External	The user acquired the role outside Oracle Applications Cloud.

15 Reporting on Application Users and Roles

Run the User Details System Extract Report

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

Related Topics

- User Details System Extract Report Parameters
- User Details System Extract 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.

Parameters

User Population

Enter one of the values shown in this table 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 the values shown in this table to identify the user-account status.

Value	Description
A	Include users with active accounts.
I	Include users with inactive accounts.
All	Include both active and inactive user accounts.

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report

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.

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.

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.

Organizations
A resource group.

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

Managers
The manager of a resource group.

Start Date
The account's start date.

Created By
The user name of the user who created the account.

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report Parameters

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 the history of a specified Oracle Fusion Cloud HCM user account. To run the reports, you must inherit the ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI duty role.

Several predefined job roles, including IT Security Manager and Human Resource Specialist, inherit this duty role. To run the reports:

1. Open the Reports and Analytics work area.
2. Select **All Folders** > **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. Click the **Person User Dashboard** entry.
2. On the Person User Summary page, complete the parameters shown in this table to filter the report and click **Apply**.

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

3. When 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**.
2. On the Person User Detail page, complete either or both of the parameters shown in this table and click **Apply**:

Parameter	Description
Start Date	The user's start date. Users with start dates equal to or later than this date may appear in the report.
Person ID	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** .

Related Topics

- User History Report

User History Report

This topic describes the User History report, which extracts and formats the history of a specified Oracle Fusion Cloud HCM user account. Oracle Support may ask you to run this report to help diagnose user-related errors.

To run the report, you must inherit the ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI (Manage Users) duty role. Several predefined job roles, including IT Security Manager and Human Resource Specialist, inherit this duty role. Follow these steps to run the report.

1. Select **Navigator** > **My Team** > **Users and Roles**.
2. On the Search Person page, search for the person of interest.
3. In the search results, click the person name to open the Edit User page.
4. On the Edit User page, click **Print User History**. In the User History dialog box, you can review the report.

   You can either print the report or download a PDF file by clicking relevant icons in the User History dialog box.
5. Click **Cancel** to close the User History dialog box.

> **Tip:** You don't have to view the report. You can select **Print User History** > **Download** to download the PDF file. The file name is in the format **<person ID>_UserHistory.pdf**.

This report is identical to the Person User Information report, which authorized users can run in the Reports and Analytics work area.

Report Contents

For the selected user, the report includes:

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

View Role Information Using Security Dashboard

As an IT Security Manager, you can use the Security Dashboard to get a snapshot of the security roles and how those roles are provisioned in the Oracle Cloud Applications.

The information is sorted by role category and you can view details such as data security policy, function security policy, and users associated with a role. You can also perform a reverse search on a data security policy or a function security policy and view the associated roles.

You can search for roles using the Role Overview page. You can view the count of the roles which includes the inherited roles, data security policies, and function security policies on this page. Clicking the number in a tile on this page takes you to the corresponding page in the Role Dashboard. You can view role details either on the Role Overview page of the Security Dashboard or the Role Dashboard.

You can view role information such as the directly assigned function security policies and data security policies, roles assigned to users, directly assigned roles, and inherited roles list using the Role Dashboard. Clicking any role-related link on a page of the Security Dashboard takes you to the relevant page in the Role Dashboard. You can export the role information to a spreadsheet. The information on each tab is exported to a sheet in the spreadsheet. This dashboard supports a print-friendly view for a single role.

Here are the steps to view the Security Dashboard:

1. In the Reports and Analytics work area, click **Browse Catalog**.
2. On the Oracle BI page, open **Shared Folders** > **Security** > **Transaction Analysis Samples** > **Security Dashboard**.

   All pages of the dashboard are listed.
3. To view the Role Category Overview page, click **Open**.

   The page displays the number of roles in each role category in both tabular and graphical formats.
4. In the **Number of Roles** column, click the numeral value to view the role-related details.
5. Click **Role Overview** to view the role-specific information in the Role Dashboard.

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. 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 shown 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 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 Fusion Cloud HCM. 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 shown 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.

Parameter	Description
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

Scheduling the Import User Login History process to run daily is a prerequisite to get a valid report about inactive users.

The Import User Login History process imports information that the Inactive Users Report process uses to identify inactive users. The Inactive Users Report process helps to identify users who haven't signed in for a specified period.

Before you run the inactive users report for a certain period, make sure that the Import User Login History data exists for that period. It's important to know when the user last signed in. That's why it's recommended to always run the Import User Login History process for a longer duration to offer greater flexibility with the date range.

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **Inactive Users Report** process.
3. In the Process Details dialog box, set parameters to identify one or more users.
4. 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

> **Note:** The information in the report relating to the user's latest activity isn't based solely on actions performed by the user in the UI. Actions performed on behalf of the user, which create user sessions, also affect these values. For example, running processes, making web service requests, and running batch processes are interpreted as user activity.

Related Topics

- Schedule the Import User Login History Process

User Role Membership Report

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

To run the report process:

1. Open the Scheduled Processes work area.
2. 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** process.
3. In the Process Details dialog box, set parameters and click **Submit**.
4. Click **OK** to close the confirmation message.

> **Note:** Only the roles at the top of a role hierarchy are included in the Role Name column of the All roles report. If you want to review a role that is lower down the role hierarchy, then apply a filter for the role in which you're interested, to the Inherited Role Hierarchy column.

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 all 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 all 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 **Data Security Policies** to view the data security report for any population. If you leave the option deselected, then only the function security report is generated.

> **Note:** If you don't need the data security report, then leave the option deselected to reduce the report processing time.

Debug

Select **Debug** to include the role GUID in the report. The role GUID is used to troubleshoot. Select this option only when requested to do so by Oracle Support.

Viewing the Report Results

The report produces either one or two .zip files, depending on the parameters you select. When you select **Data Security Policies**, two .zip files are generated, one for data security policies and one for 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.

This table shows the file prefix values for each report type.

Report 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 report type.

Report Type	File Suffix	File Format	File Contents
Any	DataSec	CSV	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when **Data Security Policies** is selected. **Note:** Extract the data security policies only when necessary, as generating this report is time consuming.
Any	Hierarchical	CSV	Functional security policies in a hierarchical format. The .zip file

Report Type	File Suffix	File Format	File Contents
			contains one file for each user or role.
• **Multiple users** • **All roles**	CSV	CSV	Functional security policies in a comma-separated, tabular format.

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. Open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the **User Password Changes Audit Report** process.
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.
  - REST_API means that the change was made for the user by SCIM REST APIs.
- The date and time of the change. The format of date and time of the change is "dd/MM/yyyy HH:mm:ss".

View Locked Users and Unlock Users

A user gets locked in the application on entering incorrect password for multiple times. The locked users report provides the list of locked users for both these scenarios.

You can get a list of locked users using the Locked Users scheduled process. You can then manually unlock the users using the Security Console. Only an administration user with the IT Security Manager job role can run the locked users report.

View Locked Users

1. In the Scheduled Processes work area, click **Schedule New Process**.

2. Search and select the **Locked Users** process and click **OK**.
3. In the Process Details dialog box, click **Submit**.
4. Click **OK** in the confirmation message dialog box.
5. Click **Succeeded** for the selected Locked Users report.
6. In the **Log and Output** section, click **Attachment** to download the report spreadsheet.

   The spreadsheet shows the list of users who are locked.

The Locked Users spreadsheet contains the following two tabs:

- LOCKED_USERS_<RequestID> - This tab contains the list of locked and active users who can't sign in to the application because of locked status.
- LOCKED_AND_INACTIVE_USERS_<RequestID> - This tab contains list of locked and inactive users who can't sign in to the application because of locked and inactive status.

Unlock Users

1. On the Security Console, click **Users**.
2. From the **Search** drop-down list, select **Locked Users** and click the search icon.

   All the locked users are displayed.
3. Click the display name of a user to view the details.
4. Click **Edit**.
5. In the Account Information section, deselect **Locked**.
6. Click **Save and Close**.
7. Click **Done**.

   The user is unlocked and can sign in to the application.

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.

Related Topics

- User Details System Extract Report

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.

16 HCM Data Roles and Security Profiles

HCM Data Roles

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. After implementation, you can also perform this task in the Workforce Structures work area. The **Assign Security Profiles to Role** task opens the Manage Data Roles and Security Profiles page. You must have the IT Security Manager job role to perform this task.

Job Role Selection

When you create an HCM data role, you include a job role. The secured 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.

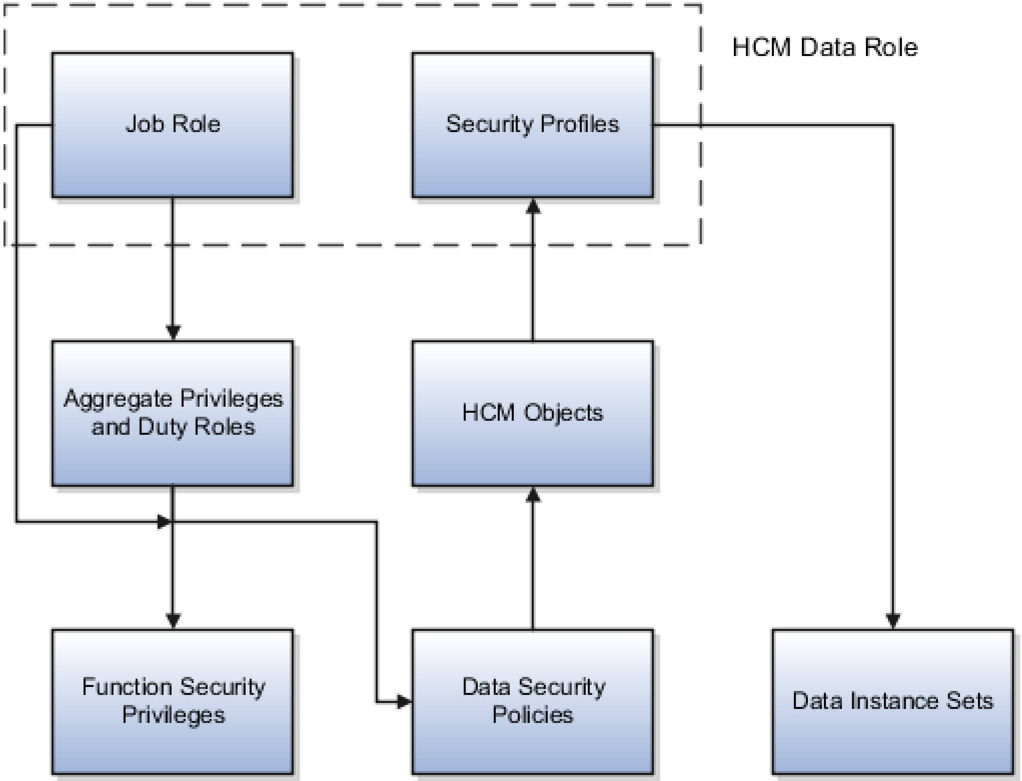
> **Note:** You must ensure that the job role doesn't have directly assigned security profiles. Search for the job role on the Manage Data Roles and Security Profiles page. In the search results, confirm that no check mark appears in the **Security Profiles Assigned** column. If security profiles are assigned to the job role, then you must revoke them before including the job role in an HCM data role. You can reassign the security profiles to the job role after creating the 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 might 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. This figure shows these components of the HCM data role.



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.

Related Topics

- HCM Security Profiles
- Best Practices for HCM Data Roles and Security Profiles
- How do I provision HCM data roles to users?

HCM Security Profiles

Security profiles identify instances of Human Capital Management (HCM) objects. For example, a person security profile identifies one or more Person objects, and a payroll security profile identifies one or more Payroll objects.

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. You're recommended not to assign security profiles directly to job roles.

HCM Object Types

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

- Country
- Document Type
- Job Requisition
- Legislative Data Group (LDG)
- Organization
- Payroll
- Payroll Flow
- Person
    - Managed Person
    - Public Person
- Position
- Talent Pool
- Transaction

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.

Predefined security profiles provide view-all access to secured objects. For example, the View All Positions security profile provides access to all positions in the enterprise.

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.

Enable access to future-dated objects as follows:

- For organizations, select the **Include future organizations** option in the organization security profile
- For positions, select the **Include future positions** option in the position security profile

- For person records, select the **Include future people** option in the person security profile

> **Tip:** The predefined View All Workers security profile doesn't provide access to future-dated person records. The predefined View All People security profile, which provides access to all person records, including those of contacts, does provide access to future-dated records.

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 or Workforce Structures work area.

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.

Related Topics

- Predefined HCM Security Profiles
- Best Practices for HCM Data Roles and Security Profiles

Predefined HCM Security Profiles

The Oracle Human Capital Management Cloud security reference implementation includes the predefined HCM security profiles shown in this table.

Security Profile Name	Security Profile Type	Data Instance Set
View All Countries	Country	All countries in the FND_TERRITORIES table
View All Document Types	Document Type	All administrator-defined document types in the enterprise
View All Flows	Payroll Flow	All payroll flows in the enterprise
View All Job Requisitions	Job Requisition	All job requisitions in the enterprise
View My Team’s Requisitions	Job Requisition	Job requisitions for my team or my subordinates

Security Profile Name	Security Profile Type	Data Instance Set
View All Legislative Data Groups	LDG	All LDGs in the enterprise
View All Organizations	Organization	All organizations in the enterprise
View All Payrolls	Payroll	All payrolls in the enterprise
View All People	Person	All person records in the enterprise
View All Positions	Position	All positions in the enterprise
View All HCM Transactions	Transaction	All HCM transactions on the Transaction Console
View All Transactions	Transaction	All transactions on the Transaction Console
View All Workers	Person	The person records of all people with currently active or suspended assignments in the enterprise
View Manager Hierarchy	Person	The signed-in user's line manager hierarchy
View Own Record	Person	The signed-in user's own person record and the person records of that user's contacts
View All Talent Pools	Talent Pool	All private and nonprivate talent pools
View All Public Talent Pools	Talent Pool	All nonprivate talent pools
View By Ownership	Talent Pool	Talent pools for which the user is the named owner

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.

Create an HCM Data Role

The data role lets HR specialists access person records based on their areas of responsibility. In this example, you create an HCM data role that you can assign to all human resource (HR) specialists in Vision Corporation.

For example, an HR specialist could be the human resources representative for the Vision Canada legal employer. Using this data role, the HR specialist could access person records for workers in Vision Canada.

Before You Start

You need to do a couple of things first:

1. Define an area of responsibility for each HR specialist. Select the **Human resources representative** responsibility type and set the scope to the relevant legal employer, for example, Vision Canada.
2. Check that security profiles aren't assigned directly to the Human Resource Specialist job role. If they are, then you must remove them. Otherwise, the HR specialist's access to person records may not be as expected.

Create the HCM Data Role

Let's look at how you enter the key values for this data role. For other fields, you can use the default values.

1. Select **Navigator** > **My Client Groups** > **Workforce Structures**.
2. On the Tasks panel tab of the Workforce Structures work area, select **Manage Data Roles and Security Profiles**.
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, enter these values.

Field	Value
Data Role	Legal Employer HR Specialist
Job Role	Human Resource Specialist

5. Click **Next** to open the Create Data Role: Security Criteria page.

Specify Security Criteria for Each Secured Object

1. In the Person section, enter these values.

Field	Value
Person Security Profile	Create New
Name	Workers by Legal Employer

2. Select **Secure by area of responsibility**.
3. For all other security profiles, select a supplied View All profile. For example, in the Public Person section select **View All People**, and in the Position section, select **View All Positions**.
4. Click **Next** until you reach the Assign Security Profiles to Role: Person Security Profile page.

Create the Person Security Profile

1. In the Area of Responsibility section, select **Secure by area of responsibility** if it isn't already selected.

2. Enter these values.

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

3. Click **Review** to open the Create Data Role: Review page.

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, you can search for the new HCM data role to confirm that it was created successfully. When the roles's status is **Complete**, you can assign the role to your HR specialists.

Best Practices for HCM Data Roles and Security Profiles

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 might 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.

Assigning Duty Roles to Data Roles

Duty roles and aggregate privileges should not be directly added to the HCM Data Role through Security Console. You're recommended to add them only to the underlying job role that's inherited by the HCM Data Role.

Related Topics

- Configure HCM Data Roles and Security Profiles for Audit

Regenerate Security Profiles

A new feature might require you to update some existing custom security profiles to use the feature. You only need to regenerate a security profile when it's required for a new feature. This info is in the What's New document for a release.

Regenerating Security Profiles Individually

You can regenerate a single security profile by editing the profile and then saving it. For example, if you need to regenerate a custom document type security profile, use the **Edit Document Type Security Profiles** page to make a minor update to the definition of the security profile and then save it.

Regenerating Multiple Security Profiles

You can use the **Regenerate Data Security Profiles** process to regenerate all of your custom security profiles for any of the following security profile types:

- Document type security profiles
- Job Requisition Security Profile

- Legislative data group (LDG) security profiles
- Organization security profiles
- Payroll Security Profile
- (Payroll) Flow Pattern Security Profile
- Person security profiles
- Position security profiles
- Transaction Security Profile

You only need to run this process when it's required for a new feature. To run the Regenerate Data Security Profiles process, follow these steps:

1. Sign in with the following roles or privileges:
    - IT Security Manager
    - Human Capital Management Application Administrator
2. Open the Scheduled Processes work area.
3. In the Scheduled Processes work area, click **Schedule New Process**.
4. In the Schedule New Process dialog box, search for and select the **Regenerate Data Security Profiles** process.
5. Click **OK**.
6. In the Process Details dialog box, select the type of security profiles to regenerate.
7. Click **Submit**.

The generated log file lists the name of each regenerated security profile, along with a time stamp. This lets you know how long it took to regenerate each security profile.

> **Note:** You should not schedule this process, as that could lead to unintended changes in the data. If you used the Security Console to update a condition that was generated for a security profile, this process will overwrite that custom SQL definition according to how it's defined on the respective security profile page.

Role Delegation

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** > **Me** > **Roles and Delegations**.

You can also make a role delegable by using the **Security Console**. In the **Users** tab, search and view the selected user account details and edit. In the roles table there is an **Assignable** option for each role listed. Once the **Assignable** option is checked on the role, the role becomes delegable. Click **Save and Close**.

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 extra 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.

> **Note:** The role may have been autoprovisioned to you based on your assignment attributes. If the relevant assignment has a future termination date, then you can't delegate the role. This restriction doesn't apply to the proxy user, whose assignments can have future-dated terminations.

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.

If you have the Human Resource Specialist job role, you can use the Manage User Account page to delegate roles that are allowed for delegation on behalf of another selected user. The proxy user can see all delegations and who made them on their user account page, but they can't edit or delete delegations performed by others.

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 data access 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 the role isn't provisioned again. However, 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 by month which manager hierarchies the proxy can access.

Month	Manager 1 Hierarchy	Manager 2 Hierarchy	Manager 3 Hierarchy
January	Yes	No	Yes
February	Yes	Yes	Yes

Month	Manager 1 Hierarchy	Manager 2 Hierarchy	Manager 3 Hierarchy
March	No	Yes	Yes
April	No	No	Yes

For example, the proxy can access the hierarchies of all three managers in February. 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.

Limit the Delegation Duration

You can specify the maximum number of days of the duration of role delegations using a predefined profile option. Once specified, the end date for a role delegation is required. If users try to save a role delegation without setting a valid end date, then an error message alerts them to the latest allowable date for the end date.

To set the profile option, follow these steps:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, enter PER_USER_DELEGATION_MAX_DAYS in the **Profile Option Code** field and click **Search**.
3. In the Profile Values section of the search results, enter the number of days for the duration of delegation in the **Profile Value** field.
4. Click **Save and Close**.

The default profile value is 0, which specifies that the end date for a role delegation is not validated.

Notifications Support in Role Delegation

When a role delegation is created or deleted, you can choose to send a notification that indicates the creation or deletion. Introducing a notification upon creating or deleting a delegation notifies users that they have may have new or different responsibilities.

When an employee (Delegator) creates or deletes a delegation (Self-Service), a notification is sent to the user defined as the Proxy (Delegate To). When an HR Administrator creates or deletes a delegation (On-Behalf of), a notification is sent to both the selected person on behalf of whom the delegation was created or deleted (Delegator), and the user defined as the Proxy (Delegate To).

You enable this feature by setting the delivered PER_USER_DELEGATION_SEND_NOTIFICATIONS profile option to Y.

To enable the profile option, navigate to the Setup and Maintenance work area:

1. Search for and click the Manage Administrator Profile Values task.
2. Search for and select the profile option.
3. Click to add a new Profile Value.
4. Select the Level as Site.
5. Enter a Y in the Profile Value field.
6. Click Save and Close.

The default profile value is 0, which will not send notifications.

Related Topics

- How You Enable Delegation for a Role

Configure Access to List of Proxy Users in Role Delegation

The data security policies that contain the Choose Proxy for Role Delegation privilege secure the list of values using the public person security profile. By default, the list of values shows the people in that public person security profile.

In this example, you learn how to create a data security policy to limit the list of values to a user's peers and management hierarchy.

The following table summarizes the key decisions for this scenario.

Decisions to Consider	In This Example
What is the name and display name of the database resource condition for proxy users?	Peers and Above and Peers and Above
How will the database resource conditions be specified?	SQL predicate

Decisions to Consider	In This Example
Which workers should appear in the list of proxy users?	The peers and management hierarchy of the delegator.

Summary of the Tasks

Enable access to a restricted list of proxy users by:

1. Creating a database resource condition.
2. Editing the Employee role to end date existing data security policy.
3. Creating replacement data security policy for the Employee role that references the new database resource condition.

Create a Database Resource Condition

You create a database resource condition that you will include in data security policy.

1. Select **Navigator** > **Tools** > **Security Console**.
2. On the Security Console, click the Administration tab.
3. On the General subtab, click **Manage Database Resources**.
4. On the Manage Database Resources and Policies page, enter **PER_PERSONS** in the **Object Name** field and click **Search**.
5. In the Search Results section, click the **Edit** icon.
6. On the Edit Data Security: PER_PERSONS page, click the Condition tab.
7. On the Condition tab, click the **Create** icon.
8. In the Create Database Resource Condition dialog box, complete the fields as shown in the following fields:

Field	Value
Name	Peers and Above
Display Name	Peers and Above
Condition Type	SQL predicate

In the **SQL Predicate** field, enter the following statement:

```
&TABLE_ALIAS.PERSON_ID in (select manager_id from per_manager_hrchy_dn
where person_id = NVL(HRC_SESSION_UTIL.GET_USER_PERSONID,-1)
and trunc(sysdate) between effective_start_date and effective_end_date
and manager_type = 'LINE_MANAGER' UNION
select b.person_id from per_assignment_supervisors_f a, per_assignment_supervisors_f b
where a.person_id = NVL(HRC_SESSION_UTIL.GET_USER_PERSONID,-1)
and trunc(sysdate) between a.effective_start_date
and a.effective_end_date and a.manager_type = 'LINE_MANAGER'
and a.manager_type = b.manager_type and a.manager_id = b.manager_id
and a.person_id != b.person_id
and trunc(sysdate) between b.effective_start_date and b.effective_end_date)
```

9. Click **Save**.

End Date the Data Security Policy Granted to the Employee Abstract Role

You edit the Employee role to end date the existing data security policy.

1. Click the **Roles** tab on the **Security Console**.
2. Search for and select the Employee role.
3. In the search results, select **Edit Role** on the role's **Actions** menu.
4. On the **Basic Information** page, click the **Data Security Policies** train stop.
5. In the **Privilege** search field, enter **Choose Proxy** and press **Enter**.
6. In the row containing the specified privilege for the Public Person data resource, select **Edit Data Security Policy** on the **Actions** menu.
7. In the Edit Data Security Policy dialog box, enter today's date in the **End Date** field.
8. Click **OK** to close the Edit Data Security Policy dialog box.

   Remain on the **Data Security Policies** page.

Create Data Security Policy

You create a new data security policy that provides restricted access to proxy users for your Employee role.

1. On the **Data Security Policies** page, click **Create Data Security Policy**.
2. Complete the fields in the Create Data Security Policy dialog box using the values shown in this table.

Field	Value
Policy Name	Restricted Access to Proxy Users Policy
Database Resource	Public Person
Data Set	Select by instance set
Condition Name	Peers and Above
Actions	Choose Proxy for Role Delegation

3. Click **OK**.
4. Click the **Summary** train stop.
5. Click **Save and Close** to save your changes to the Employee role.

How You Enable Delegation for a Role

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. You can use:

- The **Assign Security Profiles to Role** task in the Setup and Maintenance work area

- The **Manage Data Roles and Security Profiles** task in the Workforce Structures work area

You must have the IT Security Manager job role to manage role delegation.

The following delegation scenarios are typical:

- Employees can delegate their own roles.
- Human Resource Specialists can delegate roles **on behalf** of employees.

To disable **on behalf delegation** for Human Resource Specialist role, you must remove the Manage Role Delegations aggregate privilege from that role.

> **Note:** You must evaluate the impact of enabling delegation for each role. Some roles, such as IT Security Manager, are sensitive and grant wide ranging access to highly restricted information. Such roles must only be granted to select individuals in the organization and should never be set up as delegation-enabled. Before enabling delegation on a role, you should carefully assess the downstream implications of doing so. Periodical review of sensitive roles is recommended to ensure that delegation has not been accidentally granted.

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.

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.

Auditing the Role Delegation

It is recommended to turn on auditing on the delegated role business object. You can choose to retrieve audit information either on Role Delegated to Proxy or Role Delegated by Delegator. Find out more about setting up and using the audit in the topic *How You Audit Oracle HCM Cloud Business Objects*.

It is recommended to enforce a periodic monitoring control to review audit logs. Such a review will help to confirm that role delegation is in line with security practices. Auditing should also be performed on changes to auditing settings, and only a limited set of users should be able to update the auditing configuration.

Delegation of Custom Job and Abstract Roles

If you create an 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 might assign the predefined **View Own Record** security profile to your custom role. Alternatively, you might 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.

Related Topics

- Role Delegation
- How You Audit Oracle HCM Cloud Business Objects

Assign Security Profiles to Job and Abstract Roles

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 have access to 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.

Assign 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. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role
2. On the Manage Data Roles and Security Profiles page, search for the job or abstract role.
3. In the search results, select the role and click **Edit**.
4. On the Edit Data Role: Role Details page, click **Next**.
5. On the Edit Data Role: Security Criteria page, select the security profiles that you want to assign to the role.
6. Click **Review**.
7. On the Edit Data Role: Review page, click **Submit**.

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

> **Note:** The role to which you're assigning security profiles may be a copy of another role with security profiles assigned. In this case, no Check mark appears in the **Security Profiles Assigned** column. However, a message warns you that the role already has data security policies from existing security profiles. The message suggests ways of removing these existing policies before proceeding. You're recommended to avoid this situation by revoking security profiles from roles before you copy them.

Revoke 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.

Related Topics

- Guidelines for Copying Abstract Roles

How You Preview HCM Data Security

On occasion, users may report problems with accessing secured data, such as person and organization records. As users typically have multiple roles, diagnosing these problems can be challenging. To help you with this task, you can use the Preview HCM Data Security interface.

Using this interface, you can analyze a user's data access based on all of their current roles and areas of responsibility. This topic explains how to use the **Preview HCM Data Security** interface in the **Workforce Structures** work area.

Watch video

Identifying the User

To start your analysis, you search for and select the user name. When you select the user, the following sections of the page are populated automatically.

Page Section	Section Contents
Currently Assigned Roles	The job, abstract, and data roles that the user currently inherits directly. This section also identifies security profiles assigned to those roles.
Currently Assigned Areas of Responsibility	Details of the user's areas of responsibility, if any. You need this information when investigating access to person or position records if that access is secured by area of responsibility.
Session-Based Roles	The roles associated with the user's latest session. Both directly and indirectly inherited roles are listed.

The user must have signed in at least once, as this information is taken from the user's latest session.

Identifying the Privileges

Most data-access problems are of one of the following types:

- The user expects to access an instance of a secured object, such as a person record, but the record isn't found.
- The user expects to perform an action, such as Promote Worker, but the action isn't available.
- The user can access an instance of a secured object, such as a person record, but the record should not be accessible.
- The user can perform an action, such as Promote Worker, but the action should not be available.

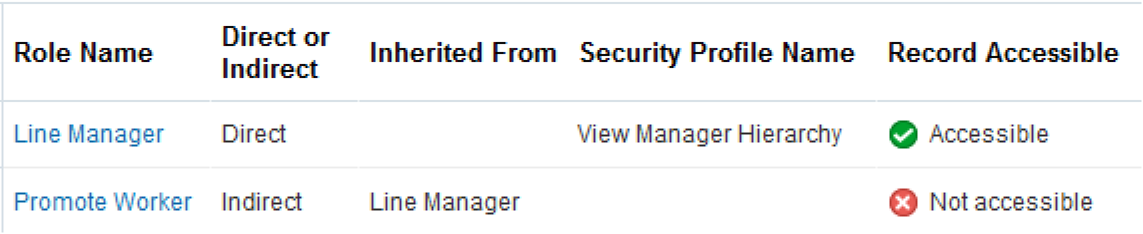
To investigate these types of problems, start by identifying what the user was trying to do. For example, the user may have found the required person record but couldn't select the Promote Worker action. You then identify the data security privilege and data resource that control this access. If you know the names of the data security privilege and data resource, then you can select them in the Access Based on Privilege section. Alternatively, you can search for the associated data security policy by aggregate privilege name, for example. When you select a value in the search results, the **Privilege** and **Data Resource** fields are completed automatically.

Previewing Access

When the fields in the Access Based on Privilege section are complete, you click **Preview Access**. The Access Verification section of the page is updated automatically to identify every instance of the data security policy that's granted to the user. In the **Verify Access For** field, you select the secured record that's the subject of this investigation and click **Verify**. For example, you select the person record of the person the user couldn't promote. The section is updated automatically to show:

- The roles to which the data security policy is granted, and how the user inherits those roles
- The security profiles, if any, assigned to those roles
- Whether the roles make the record or action accessible to the user

This figure shows typical content of the Access Verification section.



Role Name	Direct or Indirect	Inherited From	Security Profile Name	Record Accessible
Line Manager	Direct		View Manager Hierarchy	✓ Accessible
Promote Worker	Indirect	Line Manager		✗ Not accessible

When you click an instance of the role name in the Access Verification section, you see data security policy details, including the SQL predicate. The information provided by all sections of the Preview HCM Data Security page should be sufficient for you to diagnose and resolve most data-access issues.

Configure HCM Data Roles and Security Profiles for Audit

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. In the Setup and Maintenance work area, search for and click the **Manage Audit Policies** task.
2. On the Manage Audit Policies page, click **Configure Business Object Attributes** in the Oracle Fusion Applications section.
3. On the **Configure Business Object Attributes** page, select a product. For example, set **Product** to **Global Human Resources**.
4. In the **Audit** column of the table of business objects that appears, select an object. For example, select **Person Security Profile** or **Data Role**.
5. In the Audited Attributes section of the page, a list of attributes for the object appears by default. Click **Create**.

   The **Select and Add Audit Attributes** dialog box opens.
6. In the **Select and Add Audit Attributes** dialog box, you can update the default selection of attributes to audit. For example you can deselect some attributes, if appropriate. Click **OK** to close the Select and Add Audit Attributes dialog box.
7. Click **Save and Close**.
8. On the **Manage Audit Policies** page, set **Audit Level** to **Auditing** in the Oracle Fusion Applications section.
9. 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

- How You Audit Oracle HCM Cloud Business Objects
- Enable Audit for Oracle HCM Cloud Business Objects
- Auditable Oracle HCM Cloud Business Objects

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** > **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** > **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** > **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

Securing Object Name	Description
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 the diagnostic tests shown in this table by selecting Run Diagnostics Tests from the Settings and Actions menu.

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
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

Related Topics

- HCM Data Roles Configuration Diagnostic Test
- HCM Security Profile Configuration Diagnostic Test
- HCM Securing Objects Metadata Diagnostic Test

17 Person Security Profiles

Guidelines for Securing Person Records

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 with currently active or suspended assignments
- The signed-in user's own record
- Shared person information

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

> **Note:** The View All People security profile provides access to all person records, including those of contacts, for example. It also provides access to future-dated 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-dated person records.

For nonstandard requirements, create 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.

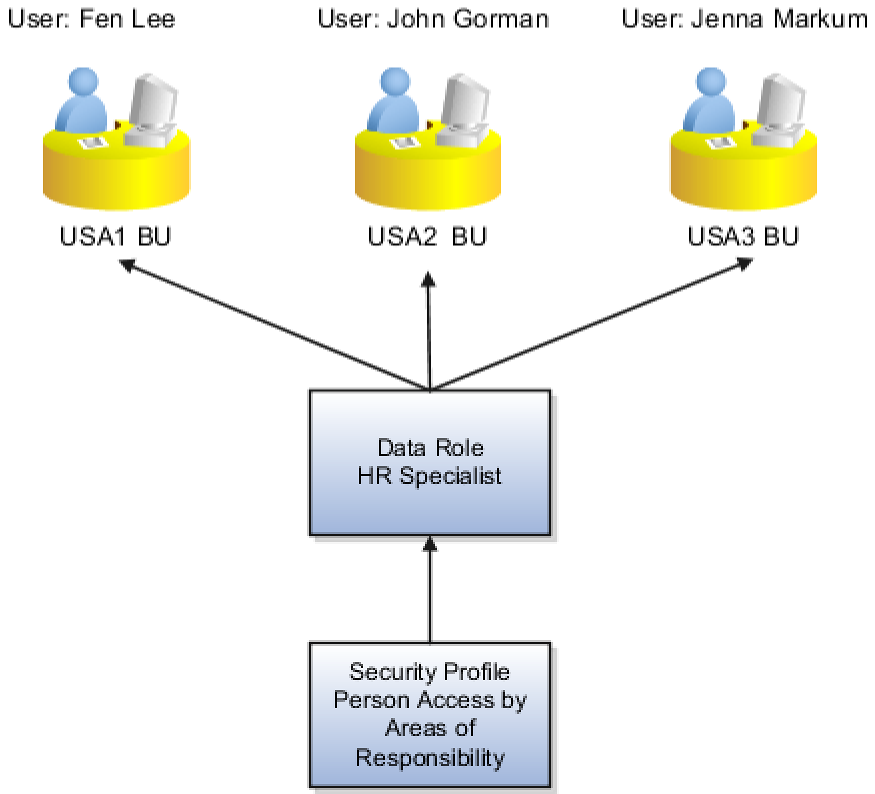
For example, consider the human resource (HR) specialists shown in this table. They perform the same job role but for workers in different business units.

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.



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.

You can also include up to three exclusion rules. These rules exclude selected person records from the set of records that the security profile identifies.

Securing Access to Imported Candidates

You can secure access to the records of candidates imported from Oracle Talent Acquisition Cloud. 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 Oracle Integration Cloud
- Fixed and Integrated with Oracle Integration Cloud

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

Related Topics

- Options for Securing Person Records by Manager Hierarchy
- How You Secure Person Records by Area of Responsibility
- Secure Person Records by Area of Responsibility

How You Secure Person Records by Area of Responsibility

When you secure person records by area of responsibility, you select a scope and a responsibility type. The scope can be either a single value, such as Job or Location, or a supplied pair of values, such as Business unit and department.

This topic explains how these scope values are matched to a user's areas of responsibility to see whether the user can access the person records.

Using a Single Responsibility Scope Value

When you select a single scope value, such as **Department** or **Country**, the user's area of responsibility needs to include that scope value. Otherwise, the user can't access relevant person records. Suppose you secure person records using these values:

- Responsibility type: Human resources representative
- Scope: Department

A user could have the four areas of responsibility shown in this table for the responsibility type.

Area of Responsibility	Business Unit	Department
1	Vision BU 1	Vision Department 1
2	Vision BU 2	None
3	Vision BU 3	Vision Department 3
4	None	Vision Department 4

This user can access person records in:

- Vision Department 1
- Vision Department 3
- Vision Department 4

But the user can't access person records in:

- Vision BU 1 if they aren't also in Vision Department 1
- Vision BU 2
- Vision BU 3 if they aren't also in Vision Department 3

Using Multiple Responsibility Scope Values

You can select a responsibility scope value that's made up of two individual values, such as **Country and department** or **Legal employer and job**. When you secure person records using one of these paired values, the user's area of responsibility must include both values. Otherwise, the user can't access relevant person records. Suppose you secure person records using these values:

- Responsibility Type: Human resources representative
- Scope: Business unit and department

A user could have the four areas of responsibility shown in this table for the responsibility type.

Area of Responsibility	Business Unit	Department
1	Vision BU 1	Vision Department 1
2	Vision BU 2	None
3	Vision BU 3	Vision Department 3
4	None	Vision Department 4

This user can access person records in:

- Vision BU 1 that also belongs to Vision Department 1
- Vision BU 3 that also belongs to Vision Department 3

But the user can't access person records in:

- Vision BU 2
- Vision Department 4
- Vision BU 1 if they don't also belong to Vision Department 1 or have no department
- Vision BU 3 if they don't also belong to Vision Department 3 or have no department
- Vision Department 1 if they aren't also in Vision BU 1
- Vision Department 3 if they aren't also in Vision BU 3

The user's area of responsibility could include not only Vision BU 1 and Vision Department 1 but also Vision Location 1. The user can still access the person records because the condition in the person security profile is met. But to enforce all three conditions or secure person records using pairs of values that aren't delivered, you have to create custom criteria. For example, to secure person records using a combination of country, department, and job, you would have to use custom criteria.

> **Tip:** To exclude some person records from the records you identify by area of responsibility, you can use an exclusion rule. You don't have to define custom criteria to exclude records.

Related Topics

- Secure Person Records by Area of Responsibility

Secure Person Records by Area of Responsibility

Usually, you secure access to person records by either manager hierarchy or area of responsibility. This topic describes how to use area of responsibility.

> **Note:** If you're going to use area of responsibility, then the employees who need to access person records must have areas of responsibility defined. Let's say that your human resource specialists manage person records for a country. They must have an area of responsibility, such as human resources representative, for that country.

Create the Person Security Profile

1. Select **Navigator** > **My Client Groups** > **Workforce Structures**.
2. On the Tasks panel tab of the Workforce Structures work area, select **Manage Person Security Profile**.
3. On the Manage Person Security Profiles page, click **Create**.
4. In the Basic Details section of the Create Person Security Profile page, give the security profile a name.
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.

   You can select a single value, such as **Department** or **Job**. Or, you can select a combined value, such as **Business unit and job** or **Legal employer and location**.

   > **Note:** The **Country** scope of responsibility means the country of the legal employer, not the country where the employee assignment is based.

8. Update the worker type selections as needed. For example, to give access to just employee records, deselect all values except **Employees**.
9. So far, in the Area of Responsibility section you have identified some person records. To exclude some of those records from the security profile, select **Apply exclusion rules** in the Exclusion Rules section.
10. Click the **Add Row** icon.
11. Select an exclusion rule.

    > **Tip:** Make sure that the rule is enabled. It has no effect if it's disabled.

    You can add up to three exclusion rules.

12. Click **Next**.

Preview the Person Security Profile

On the Create Person Security Profile: Preview page, you can test your security profile before you save it.

1. On the Person Access Preview tab, select a user with the area of responsibility that you included in the security profile. When you click **Preview**:
   - The User Summary section of the page shows how many person records this user could access.
   - The Assigned Areas of Responsibility section of the tab lists the user's areas of responsibility.

   > **Note:** The results from the Person Access Preview are based on this person security profile only. Users could have other 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 see whether the user could access them. The search is of the person records that were identified when you clicked **Preview** for the user. For example, if the preview identified 50 person records, then those 50 person records are searched.
3. To view the SQL predicate that the security profile generates, click the SQL Predicate for Person Access tab.
4. Click **Save and Close** when you're done.

Related Topics

- Guidelines for Securing Person Records
- How You Secure Person Records by Area of Responsibility
- Create an HCM Exclusion Rule
- How You Assign Areas of Responsibility

Create an HCM Exclusion Rule

You can use HCM exclusion rules in person security profiles to exclude some records. For example, you could use an HCM exclusion rule to exclude person records if they're in the HR department or a particular manager hierarchy.

1. Select **Navigator** > **My Client Groups** > **Workforce Structures**.
2. On the Tasks panel tab of the Workforce Structures work area, select **Manage HCM Exclusion Rules**.
3. On the Manage HCM Exclusion Rules page, click **Create**.
4. On the Create HCM Exclusion Rule page, give the rule a name and leave **Enabled** selected.

   > **Tip:** An exclusion rule is ignored in a person security profile if it isn't enabled.
5. In the Exclusion Definition section, select an **Exclude By** value.
6. If you select a list value, then you list the objects that you want to exclude. Suppose you select **Department list**. In the Departments section, you:
   a. Click **Add**.
   b. Select a department to exclude in the **Department** field.
   c. Click **OK**.

   To add more departments to the list, just repeat these steps.
7. If you select **Department hierarchy**, then in the Department Hierarchy section you:
   a. Select the department hierarchy tree in the **Tree Name** field.

   b. Select the top department in the hierarchy in the **Top Department** field.
   c. Click **OK**.
8. If you select **HCM position hierarchy**, then you select the top position in the Position Hierarchy section.
9. If you select **Supervisor hierarchy**, then you select the top manager in the Manager Hierarchy section.

   > **Tip:** For all hierarchies, the exclusion rule includes the top node.

10. If you select an attribute value, such as **Department attribute**, then select values for the **Attribute**, **Operator**, and **Value** fields in the Exclusion Condition section. For example, you could select these values.

Attribute	Value
Attribute	Department set
Operator	Equals
Value	EMEA Set

    The attributes include some core attributes for the object plus any configured flexfield attributes.
11. Click **Save and Close** when you're done.

Now that you have an exclusion rule, you can include it in a person security profile when you secure the records by area of responsibility.

Options for Securing Person Records by Manager Hierarchy

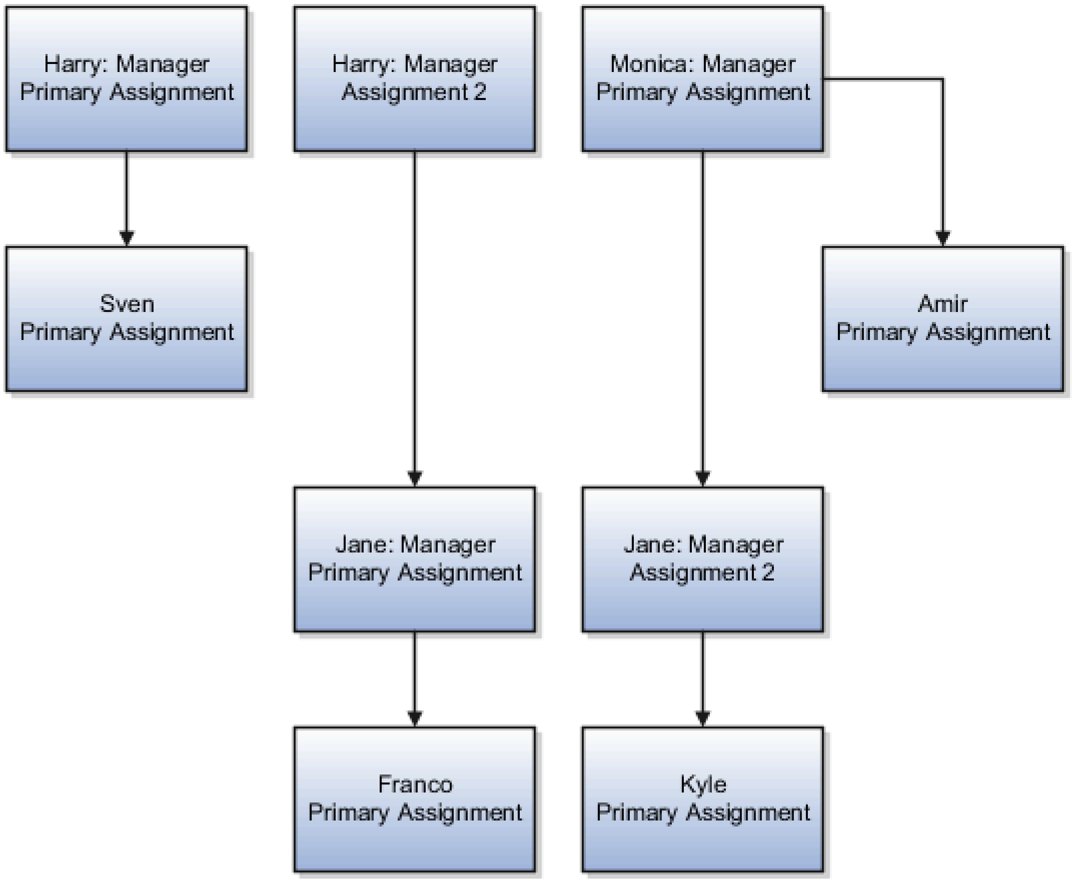
The person records that a manager can access depend on how you specify the manager hierarchy in the person security profile. This topic describes the effect of the Person or Assignment Level option, which you set to either Person or Assignment.

> **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. This figure shows this example manager hierarchy.


Harry: Manager Primary Assignment
Harry: Manager Assignment 2
Monica: Manager Primary Assignment
Sven Primary Assignment
Amir Primary Assignment
Jane: Manager Primary Assignment
Jane: Manager Assignment 2
Franco Primary Assignment
Kyle 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 configuration 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	No
Monica	No	Yes	Yes	Yes	Yes
Jane	No	No	Yes	Yes	No

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

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

Manager	Sven	Jane	Franco	Kyle	Amir
Harry	Yes	Yes	Yes	No	No
Monica	No	Yes	No	Yes	Yes
Jane	No	No	Yes	Yes	No

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.

Access to Terminated Workers

Line managers automatically lose access to terminated workers in their manager hierarchies on the day following the termination date.

Related Topics

- Manager Type in Person Security Profiles
- The Manager Hierarchy: How It's Maintained

Manager Type in Person Security Profiles

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. 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 configuration 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 **Navigator** > **My Team**, for example.

Hierarchy Content in Person Security Profiles

The Hierarchy Content attribute in a person security profile controls how access to manager hierarchies is delegated, either when you secure access to person records by manager hierarchy, or delegate a role that includes the person security profile.

To create a person security profile, use the **Manage Person Security Profile** task in the Setup and Maintenance work area.

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. 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.

Person Type in Person Security Profiles

You can secure access to person records based on either their system person type or their user person type. For example, you can secure access to the person records of workers whose system person type is Employee.

When you secure by person type, you can access the person records of workers with active or suspended assignments only. You can't access the person records of terminated workers. This topic explains the effect of the Access value when you secure access to person records by person type.

Restricted Access

When you secure by person type and set **Access** to **Restricted**, any other criteria in the security profile also apply. For example, you can select the values shown in this table:

Type	System Person Type	Access
System person type	Employee	Restricted
System person type	Contingent worker	Restricted

If you also secure access to person records by manager hierarchy in the same person security profile, then both sets of criteria apply. That is:

- The users can access the person records of employees and contingent workers in their reporting hierarchy.
- The users can't access person records of other types in the reporting hierarchy or person records outside the reporting hierarchy using this person security profile.

All Access

When you secure by person type and set **Access** to **All**, the other criteria in the security profile have no effect. For example, if you set **System Person Type** to **Employee** and **Access** to **All**, then users can access all employees in the enterprise. Other criteria in the security profile, if any, are ignored for the selected worker type.

Include Shared People Information in a Person Security Profile

A person security profile with the **Include shared people information** attribute enabled allows the user to access a person whose information is shared with them using the Share Data Access action.

For example, Joe who is a line manager uses the Share Data Access action to give Bob access to Sally's data, who reports to him. Sally is in the Milwaukee location. There is a Person Security Profile that gives access to all assignments in the Chicago location. A task that's secured with this person security profile can only see assignments in Chicago.

- If the **Include shared people information** option is enabled, Bob can use this task to access all assignments in Chicago AND all of Sally's assignments.
- If the **Include shared people information** option is disabled, Bob can use this task to access only the assignments in Chicago.

If you enable the Include shared people information attribute, ensure that you intend for the users of any tasks secured by this person security profile to have access to another person's data.

Related Topics

- How You Share Data Access With Another Person

How You Secure Access to Candidates with Job Offers in Manage Job Offer Task

Candidates with job offers from Oracle Recruiting Cloud have offer assignments in Oracle Human Capital Management Cloud. You can secure access to candidates with job offers based on these offer assignments.

Therefore, a human resource specialist, having the Address Job Offer aggregate privilege, can manage candidates with job offers securely in Oracle HCM Cloud before onboarding begins. This topic describes how to secure access to candidates with job offers.

Securing Access to Candidates with Job Offers

To secure access by area of responsibility, you select **Candidate with offer** in the Area of Responsibility section of the Create Person Security Profile page. Alternatively, you can select the **Access to candidates with offer** option in the Basic Details section of the Create Person Security Profile page. This option enables you to secure access to person records, including those of candidates with job offers, by criteria other than area of responsibility. For example, you can secure access by manager hierarchy. You can also secure access by workforce structures and global name range if those sections appear in the person security profile. The Workforce Structures and Global Name Range sections appear only if you upgraded from Release 11 to Release 12.

> **Tip:** You can't select both **Access to candidates with offer** and **Candidate with offer**. When you select **Secure by area of responsibility**, the **Access to candidates with offer** option is no longer available in the Basic Details section.

Ending Access to Candidates with Job Offers

When a candidate with a job offer becomes a pending worker, employee, or contingent worker, the offer assignment becomes inactive. You lose access to the person records of candidates with job offers when their offer assignments are inactive if:

- You can access only the inactive offer assignment, and the person security profile that secures your access evaluates active and suspended assignments only.
- Your access is secured by area of responsibility, and you don't have that responsibility for the newly hired worker.
- The candidate is a rehire, and your previous access was based on the most recently terminated assignment. You lose that access when the worker has an active assignment if you don't also have access to that active assignment.

Custom Criteria in Person Security Profiles

You can secure person records by either area of responsibility or manager hierarchy. You can also use custom criteria, in the form of SQL statements, to add to or replace the standard criteria.

Example of Using Custom Criteria

This example shows how to use custom criteria in a person security profile. In this example, the person security profile needs to include the person record of anyone who was born before 01 January, 1990.

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

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

Validating Custom Criteria

You validate custom criteria in two stages.

1. When you click **Validate** in the Custom Criteria section of the page, a syntax check runs. Any syntax errors, such as missing brackets, misspelled keywords, or single-line comments, are reported.

   > **Note:** You can include multiline comments in your SQL statements. Multiline comments start with a slash and an asterisk (/*) and end with an asterisk and a slash (*/). Single-line comments, which start with two hyphens (--), aren't valid.

2. When you click **Next** to open the Preview page, some more validation takes place and these issues are reported:
   - Use of the letter A as an alias to the ASSIGNMENT_ID attribute, because A is reserved for Oracle use
   - References to tables that include personally identifiable information (PII), which can cause runtime errors
   - Use of commands such as UNION or JOIN, which can affect performance

You need to correct any validation errors.

Defining Exceptions to Areas of Responsibility

Let's say that a user should be able to access all person records in an organization, except those in specific grades or locations. You don't have to use custom criteria to exclude some records when you secure them by area of responsibility. Instead, you can include up to three exclusion rules in the person security profile. The rules define the criteria, such as grade or location, for excluding some records.

Related Topics

- Tables and Views in Custom Criteria
- Secure Person Records by Area of Responsibility

Tables and Views in Custom Criteria

You can secure access to person records using custom criteria in the form of SQL predicates. You shouldn’t use some tables and views in custom SQL statements. They might cause runtime errors, with error message containing 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	• OKC_EMPLOYEE_CONTACT_V • OKC_SEARCH_EMPLOYEE_V • OKC_SEARCH_INT_CONTACTS_V • OKC_SIGNER_CONTACTS_V
Financials for EMEA	• JE_RU_FA_EMPLOYEE_V
General Ledger	• GL_HIERVIEW_PERSON_INFO_V
Global Human Resources	• 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_

Product	Table or View
	- 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 - 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	- PAY_AMER_W4_LOC_ADDRESS_V - PAY_AMER_W4_PERSON_ADDRESS_V

Product	Table or View
Grants Management	• GMS_ALL_CONTACTS_V • GMS_INTERNAL_CONTACTS_V
Payments	• IBY_EXT_FD_EMP_HOME_ADDR
Planning Common Components	• MSC_AP_INTERNAL_LOCATIONS_V
Profile Management	• HRT_PERSONS_D • HRT_PERSONS_X
Project Foundation	• PJF_PROJ_ALL_MEMBERS_V • PRJ_PROJECT_MANAGER_V • PRJ_TEAM_MEMBERS_F_V
Workforce Reputation Management	• 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*.

Related Topics

- Custom Criteria in Person Security Profiles
- Tables and Views for Oracle HCM Cloud

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 emails, 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.

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.

How can I exclude some records from a person security profile?

Include an exclusion rule in the person security profile. The rule uses criteria such as department or grade to identify the records to exclude.

You can secure person records in one of two ways:

- Secure by area of responsibility, or
- View all (workers with assignments).

You can include up to three exclusion rules in a person security profile. Only one of the rules can be based on a hierarchy.

What happens when I select the Access to own record check box?

When you select this check box, you can always view your own record regardless of the other criteria specified in the security profile.

If you deselect this option, then you can never view your own record regardless of the other criteria specified in the security profile.

18 Organization and Other Security Profiles

How You Secure Organizations

A valid organization security profile can secure access to all organizations in the enterprise or any subset of those organizations. This topic explains how to set the criteria in an organization security profile to identify a specific set of organizations.

You can use any combination of the following three sections of the organization security profile to identify a set of organizations:

- Organization Hierarchy
- Organization Classification
- Organization List

In the Organization List section, you can select some organizations to include and some to exclude. All criteria that you specify in all sections apply.

The following table identifies the set of organizations that results from each combination of criteria in the organization security profile.

Hierarchy	Classification	List (Exclude)	List (Include)	Set of Organizations
Yes	No	No	No	All organizations in the specified hierarchy
No	Yes	No	No	All organizations of the selected classifications in the enterprise
No	No	Yes	No	All organizations in the enterprise, minus those listed
No	No	No	Yes	The listed organizations
Yes	Yes	No	No	Organizations of the selected classifications that belong to the specified hierarchy
Yes	No	Yes	No	All organizations in the specified hierarchy, minus those listed
Yes	No	No	Yes	All organizations in the specified hierarchy, plus those listed

Hierarchy	Classification	List (Exclude)	List (Include)	Set of Organizations
No	Yes	Yes	No	All organizations of the selected classifications, minus those listed
No	Yes	No	Yes	All organizations of the selected classifications, plus those listed
Yes	Yes	Yes	No	All organizations of the selected classifications in the specified hierarchy, minus those listed
Yes	Yes	No	Yes	All organizations of the selected classifications in the specified hierarchy, plus those listed
Yes	Yes	Yes	Yes	All organizations of the selected classifications in the specified hierarchy, plus and minus those listed

The following rules apply to use of the Organization List section of the organization security profile:

- When you add an organization to the Organization List section and select **Include**, that organization is added to the security profile instance set. Typically, you do this when an organization isn't identified by the other criteria in the security profile. For example, you could include the Legal Employer classification and add a department to the Organization List section. No error would occur if you included a legal employer in the Organization List section, even though that organization was already included.
- When you add an organization to the Organization List section and select **Exclude**, that organization is excluded from the security profile instance set. Typically, you do this when an organization is identified by the other criteria in the security profile. For example, you could include a department hierarchy and add one of those departments to the Organization List section to exclude it. No error would occur if you included a legal employer in the Organization List section, even though legal employers were already excluded.

Related Topics

- Guidelines for Securing Organizations
- Examples of Organization Security Profiles

Guidelines for Securing Organizations

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.

Securing by Organization Classification

To secure access to all organizations of a single classification, select the classification in the Secure by Organization section. For example, to secure access to all legal employers in the enterprise, set the **Classification Name** in the Secure by Classification section to **Legal Employer**. You can exclude selected legal employers from this access by listing them in the Organizations section and selecting **Exclude** in the **Include or Exclude Organizations** column.

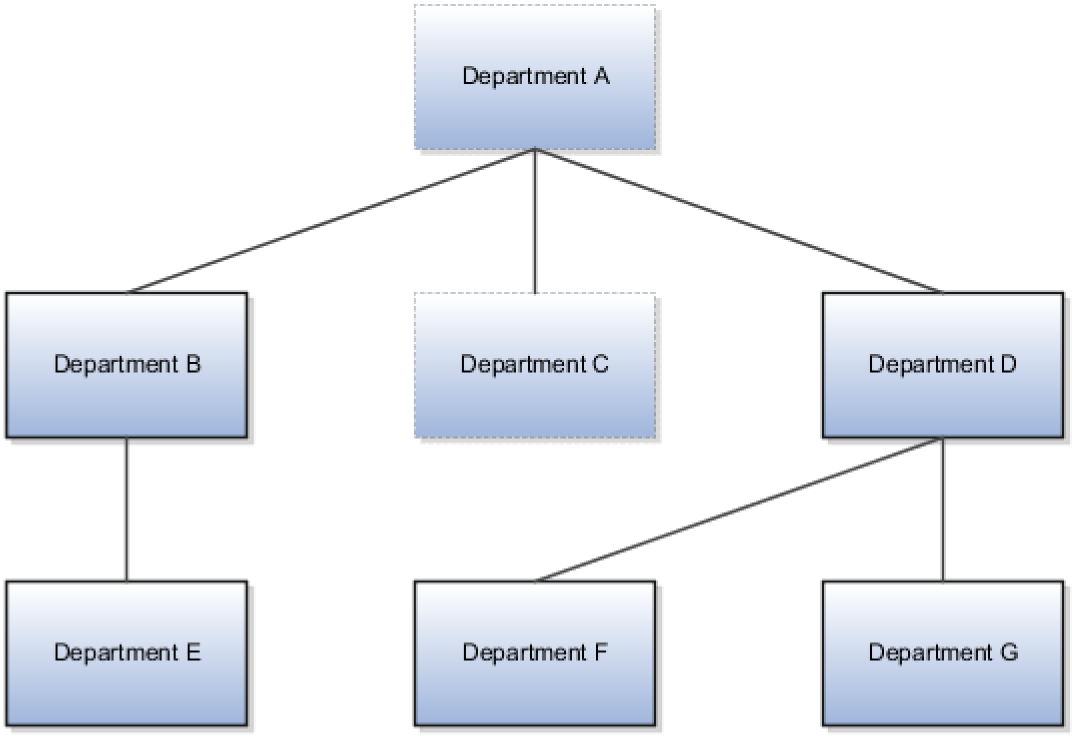
Selecting the Top Organization in an Organization Hierarchy

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 sub-hierarchies 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 belongs to the same organization hierarchy. The top organizations are therefore departments B and D, and the user's data instance set of organizations therefore includes departments B, E, D, F, and G.



Related Topics

- How You Secure Organizations
- Examples of Organization Security Profiles

Examples of Organization Security Profiles

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 hierarchy includes all types of organizations.
- 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 resources (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.

Related Topics

- Guidelines for Securing Organizations
- How You Secure Organizations

Guidelines for Securing Positions

This topic describes guidelines to consider when deciding how to secure access to position records, by securing by area of responsibility and position hierarchy. It also describes how to preview access provided by the security profile for a user before saving.

Securing by Area of Responsibility

When you secure position records by area of responsibility, the set of records that the user can access is calculated dynamically. The calculation is based on the user's assigned areas of responsibility. For example, a user may be the HR representative for a specific department. You create the position security profile based on these values. That is, you set **Responsibility Type** to **Human resources representative** and **Scope** to **Department**. In this case, any user who has that responsibility for a department can access position records defined for that department. If the user later becomes responsible for positions in a different department, then you update only that user's area of responsibility. The position security profile remains valid without update. You can also create a single data role to include the position security profile and assign it to multiple representatives. The option to secure access by position list remains available, which enables you to refine further the list of positions that users can access. For performance reasons, you're recommended to secure access to position records by area of responsibility whenever possible.

When you select the Area of Responsibility section in any position security profile, the Position Hierarchy and Workforce Structures sections become unavailable. These criteria are incompatible with securing by area of responsibility.

Securing by Position Hierarchy

Oracle HCM Cloud supports both position trees and the HCM Position Hierarchy. Depending on the values of the enterprise Position Hierarchy Configuration options, you can secure access to position records using either type of hierarchy.

> **Note:** Any future enhancements related to position hierarchies will support only the HCM Position Hierarchy. Therefore, you should consider using the HCM Position Hierarchy rather than position trees.

You set the Position Hierarchy Configuration options on the Manage Enterprise HCM Information page. They determine whether the **Position Tree** field appears in the Position Hierarchy section of the Create Position Security profile page.

- If you select only **Use HCM Position Hierarchy**, then the **Position Tree** field is hidden.
- If you select only **Use Position Trees**, then the **Position Tree** field appears.
- If you select both options, then the **Hierarchy Type** field appears, where you can select either the HCM Position Hierarchy or the position tree.

When you edit an existing position security profile, the enterprise options have no effect. If the existing position security profile is based on the position tree, then the **Position Tree** field appears. Otherwise, the **Position Tree** field is hidden.

Previewing the Security Profile

Creating a position security profile is a two-step process. Once you have defined your security criteria, you click **Next** to open the Create Position Security Profile: Preview page. Here, you can test the access provided by the security profile before you save it. On the Position Access Preview tab, you can select a user and click **Preview**. This action returns the number of position records that this security profile allows the user to access. You also see the name and type of the user's areas of responsibility, if any. You can then identify individual position records to which the security profile provides access by searching for them. The search is based on criteria such as position name, business unit, and incumbent. The search is performed within the set of position records that was returned by the **Preview** action.

You can review the automatically generated SQL predicate for your security criteria on the SQL Predicate for Position Access tab.

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

Related Topics

- Examples of Position Security Profiles
- How You Assign Areas of Responsibility

Hierarchy Content in Position Security Profiles

The Hierarchy Content section is hidden by default so you must opt-in to display it in the Position Hierarchy section. You must change the default value (N) of the profile option ORA_PER_ENABLE_POSITION_SECURITY_DELEGATION to Y to enable it.

After changing the profile option value, you must sign out and sign in to the application for the changes to take effect.

The **Hierarchy Content** attribute in a position security profile controls how access to manager hierarchies is delegated when you:

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

Create a position security profile using the **Manage Position Security Profile** task in the Setup and Maintenance work area, or by its quick action under **My Client Groups**.

Enable the **Position Hierarchy** section and choose the intended hierarchy type. Top position selection must be relative to a user's assignment to enable and select a hierarchy type.

Hierarchy Content Values

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

Value	Description
Current user's hierarchy	The position 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 user's hierarchy	The position 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 position 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.

When the line manager role is delegated to another line manager, the proxy can manage the delegator's reports. However, when viewing by position, the proxy's **My Team** information doesn't show the delegator's positions, because the manager hierarchy isn't changed by the role delegation.

> **Note:** If the proxy user's position is in the delegator's manager hierarchy, then the delegated role gives the proxy user access to his or her own position record.

Examples of Position Security Profiles

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

Human resource (HR) specialists manage position definitions for specific business units. Each HR specialist has a defined area of responsibility, where the **Responsibility Type** is set to **Human resources representative** and the business unit is selected. In the position security profile, you:

- Secure by area of responsibility.
- Set **Responsibility Type** to **Human resources representative** and **Responsibility Scope** to **Business unit**.

You can include this security profile in a data role and provision the role to any HR specialist who manages positions in a business unit.

> **Tip:** You can also secure by position list. For example, you could list positions to add to the set identified using area of responsibility.

Line Manager Who Hires Workers

Line managers in your legal employer can hire workers whose positions are below the managers' own positions in the position hierarchy. The managers' positions must be associated with active assignments. Your enterprise is using the HCM Position Hierarchy. To identify these positions, you:

- Secure by position hierarchy.
- Set **Top Position** to **Use positions from all active user assignments**.
- Deselect **Include Top Position**.

You can include this position security profile in a data role and provision the role to any line manager in your legal employer.

Related Topics

- Guidelines for Securing Positions

Document Type Security Profiles

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:** The citizenship, passports, visas and permits, and driver’s licenses that are on the **Identification Info** page (accessed through the **Identification Info** quick action) are not documents of record and access to this information is controlled using the following aggregate privileges, not document type security profiles:
>
> - Manage Person Citizenship
> - View Person Citizenship
> - Manage Person Passport
> - View Person Passport
> - Manage Person Visa or Permit
> - View Person Visa or Permit
> - Manage Person Driver License
> - View Person Driver License

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 documents of administrator-defined types in the person records that they manage.

Legislative Data Group Security Profiles

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.

Creating 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.

Transaction Security Profiles

By default, users who can access the Transaction Console can manage all transactions on the console. However, you may want to limit access so that users can manage only Talent or Compensation transactions, for example. This topic explains how to do this.

How to Secure Access to Transactions on the Transaction Console

To secure access to transactions on the Transaction Console, you have to do a few things:

1. Create transaction security profiles.

2. Create data roles and assign transaction security profiles to them.
3. Assign the data roles to users.
4. Enable transaction security.

You don't have to create the transaction security profiles separately. If you prefer, you can create them when you create the data roles. This topic explains how to create them separately, but the key steps are the same in both cases.

Creating Transaction Security Profiles

Use the **Manage Transaction Security Profiles** task to select the transaction types that users can manage. You can find this task in the Workforce Structures or Setup and Maintenance work area.

On the Create Transaction Security Profile page, you:

1. Click the **Create New** icon.
2. Set **Family** to the appropriate product family.
3. Select a category. This value identifies a category of transactions that users can manage. Categories that you don't select are excluded.
4. Optionally, select a subcategory.
    - The subcategory identifies transactions in the subcategory only. All other subcategories in the category are excluded, unless you select them separately.
    - If you select **Exclude Subcategory**, then users can manage transactions in the category, apart from those in the excluded subcategory.

You can repeat these steps to add other categories of transactions to the security profile. When you're finished, save your changes.

Creating Data Roles

To create a data role, you can use:

- The **Manage Data Roles and Security Profiles** task in the Workforce Structures work area
- The **Assign Security Profiles to Role** task in the Setup and Maintenance work area

The data role must:

- Inherit either the predefined Human Capital Management Application Administrator job role or a custom role with the required privileges.
    - The predefined Human Capital Management Application Administrator job role inherits the Review HCM Approval Transactions as Administrator duty role. You can assign this duty role to custom roles.
    - The Review HCM Approval Transactions as Business User duty role isn't inherited by any predefined role. It enables a restricted set of actions on the Transaction Console. You can assign this duty role to custom roles, such as Human Resource Specialist.
- Have an assigned transaction security profile. This security profile identifies the types of transactions that users can manage on the Transaction Console. You can:
    - Select a transaction security profile that you created using the **Manage Transaction Security Profiles** task.
    - Create a security profile in the data roles task flow.
    - Use one of the predefined security profiles, View All Transactions and View All HCM Transactions.

Create as many data roles as you need, and assign them to users. On the Transaction Console, those users can manage transactions:

- That were created by people identified by the data role's person security profile
- That belong to the categories in the data role's transaction security profile

Note that both conditions apply. You must also enable transaction security. Otherwise, users who can access the Transaction Console can manage all transactions, even if their data roles limit them to specified types of transactions.

Enabling Transaction Security

Transaction security is disabled by default. To enable transaction security, you use the **Manage Enterprise HCM Information** task. You can find this task:

- In the Workforce Structures work area
- In the Setup and Maintenance work area in the Workforce Structures functional area for your offering

Follow these steps:

1. On the Edit Enterprise page, select **Edit** > **Update**.
2. Complete the fields in the Update Enterprise dialog box and click **OK**.
3. Scroll to the Transaction Console Information section. In the Transaction Console Information section, select **Enable Transaction Security**.
4. Click **Submit**.

You have to enable transaction security once only. While it's enabled, access to transactions on the Transaction Console is secured, and users can manage only the transactions that their data roles allow.

Payroll Security Profiles

You can use different methods to provide access to payrolls for members of the Payroll department. Use the Manage Payroll Security Profiles task to organize your payroll definitions into appropriate payroll security profiles.

Then, 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

It's common to use the payroll security profile to organize payroll definitions by payroll period type. You simply create one security profile for each payroll type, such as 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 employees' work location. For example, you can create one for Canadian facilities and another for European facilities.

Individual Contributors

If your payroll managers can access only the payroll definitions that they manage, use create payroll security profiles to include only those payrolls.

Flow Security and Flow Owners

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.

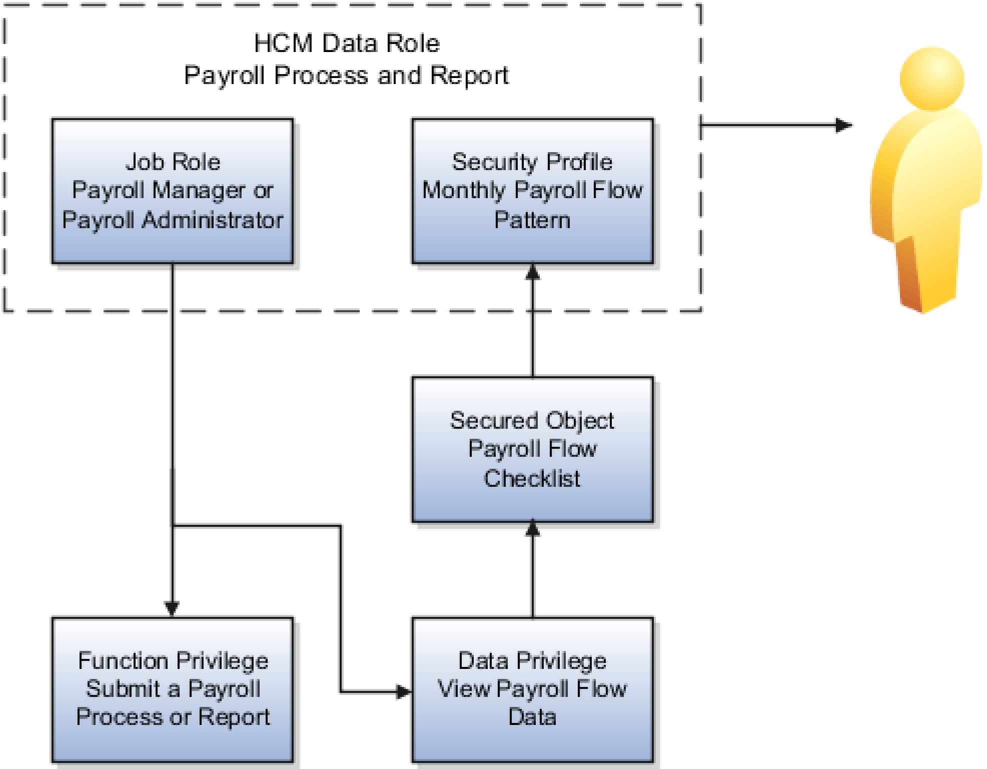
Use the Payroll Flow Security Profile task in the Setup and Maintenance work area to define security for payroll flow patterns.

Payroll Flow Security and HCM Data Roles

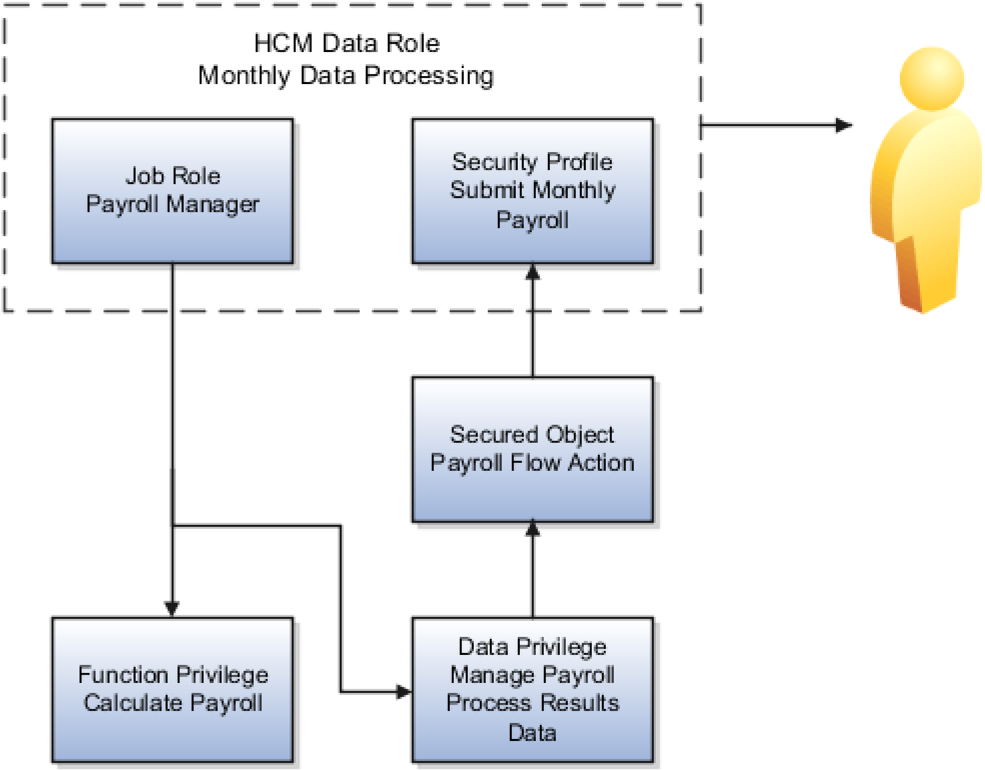
HCM data roles secure the access to flows through data privileges and to the tasks on a checklist through functional privileges.

- When you submit a flow pattern, it 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.

This 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.



The payroll manager or the payroll administrator can submit the flow and perform its tasks or have the tasks reassigned to them. The payroll manager and the payroll administrator can perform the same tasks because both of them have the same functional privileges.They can both submit and view the payroll flow data.This 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 to submit the monthly payroll flow action.



View Flow Security

When you submit a flow, you're taken to the Checklist page so that you can manage and monitor the tasks included in the flow.

You can also use the View Flows page, and navigate to these pages:

- Click on a flow to go to the Checklist page of the selected flow. The checklist page shows the list of tasks in the flow as well as their completion status.
- Click on a task to drill down to the Process Results Summary, it shows the employees processed within that task.
- Click on the employee's name to drill down to the Person Process Results page.
- Navigate from the Person Process Results page to view the detailed process results for the employee. For example, view the Statement of Earnings, Messages, Balances, and Run Results for the Calculate Payroll task.

This table shows the function privilege that secure access to the View Flow Quick Action.

View Flow Security and Privileges

Page	Aggregate Privileges	Job Roles
View Flow	Access Payroll Flow (PAY_ACCESS_PAYROLL_FLOWS)	Payroll Manager, Payroll Administrator

Access Payroll Flow aggregate privilege includes all the necessary function and data privileges to access the Checklist, Process Results Summary, and Person Results pages.

Including View Flow in Your User-Defined Role

You might have a requirement to provide access to View Flow to other job roles, to allow them to view results of specific processes. To include View Flow in a user-defined role, complete these steps.

1. Create a role by either copying a predefined job role or creating a new one.
2. Add the aggregate privilege: Access Payroll Flow.
3. Depending on the type of flow the role should have access to, you might need to provide additional function privileges such as:
    - Verify Statement of Earnings (PAY_VERIFY_STATEMENT_OF_EARNING)
    - View Employee Level Messages (PAY_VIEW_EMPLOYEE_LEVEL_MESSAGES)
    - View Payroll Balance (PAY_VIEW_PAYROLL_BALANCE)
    - View Payroll Run Results (PAY_VIEW_PAYROLL_RUN_RESULTS)
4. Create a Payroll Flow security profile to include the flows your new role should have access to.
5. Create a data role and associate the Payroll Flow security profile to it.

These aren't included in the Access Payroll Flow privileges:

- QuickPay Results: If you want to use View Flow to access the QuickPay Results, you must grant access to the QuickPay Quick Action.
- Import and Load Data: If you want to use View Flow to view results of HDL uploads, additional privileges are required.
- Ability to take action on the tasks: Actions such as Retry or Rollback aren't available.

> **Note:** If the flow-level messages aren't displayed, ensure that your data role includes this data security profile: Search Person Live Data.

Troubleshooting

If you have problems submitting or completing a task in a flow, these are the actions you can take.

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.
Can’t view or take action on a flow task submitted by another user.	Update the flow pattern to add a group to the specific task.

Examples of Flow Pattern Security Profiles

You can use different methods 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.

Scenario

Here are a few examples of payroll security profiles and data roles.

Example	Data Role	Security Profile
Payroll Processing and QuickPay Flows	Payroll Administrator	Payroll Cycle flow and the QuickPay flow
End-of -Year Reporting	Payroll Administrator	End-of -Year flow and the Archive End-of-Year Payroll Results flow
Hiring and Terminations	HR Administrator or HR Specialist	New Hire flow and the Termination flow

Talent Pool Security Profiles

You can use security profiles to control access to nonprivate talent pools.

You can control access to nonprivate talent pools in these ways:

- Assign any of the 3 delivered security profiles for talent pools to specific roles.
- Create security profiles so that only people of a specific business unit, department, or job family can access nonprivate talent pools and then assign them to the appropriate roles.

Delivered Security Profiles for Talent Pools

There are 3 delivered security profiles for talent pools:

- View All Talent Pools: Users assigned this profile can manage all private and nonprivate talent pools.
- View All Public Talent Pools: Users assigned this profile can manage all nonprivate talent pools.
- View By Ownership: Users assigned this profile can manage only talent pools for which they're the named owners. This is the default security profile.

For more information about talent pool security profiles, see the topics in the Related Topics section.

Related Topics

- Overview of Security Profiles for Talent Pools
- Create a Security Profile for Talent Pools
- Assign Talent Pool Security Profiles to Specific Roles

Create a Security Profile for Talent Pools

You can use security profiles to control access to nonprivate talent pools. You can do this on the Talent Pool Security Profiles page.

By configuring security profiles, you can ensure that only people of a specific business unit, department, or job family can access nonprivate talent pools.

1. Go to the Talent Pool Security Profiles page using one of these navigations:
    - Use the **Talent Pool Security Profiles** quick action on the My Client Groups tab.
    - Go to **My Client Groups** > **Workforce Structures** > **Talent Pool Security Profiles**.
2. On the Talent Pool Security Profiles page, click **Create**.
3. On the Create Talent Pool Security Profile page, enter a unique name for the profile.
4. To make the profile active, select the **Enabled** check box. Note that the other check boxes are disabled and you can't select them.

    You need to secure by business unit, department, or job family when you create a security profile.

5. To secure by business units:
    a. Select the **Secure by business unit** check box.

       If you opt to secure by business units, you need to select at least one business unit.

    b. Click **Add**.
    c. Search for and select the business unit that you want to include in the profile.
    d. Repeat steps 5b and 5c for all business units you want to add in the profile.
6. To secure by departments:
    a. Select the **Secure by department** check box.

       If you opt to secure by departments, you need to select at least one department.

    b. Click **Add**.
    c. Search for and select the department that you want to include in the profile.
    d. Repeat steps 6b and 6c for all departments you want to add in the profile.
7. To secure by job families:
    a. Select the **Secure by job family** check box.

       If you opt to secure by job families, you need to select at least one job family.

    b. Click **Add**.
    c. Search for and select the job family that you want to include in the profile.
    d. Repeat steps 7b and 7c for all job families you want to add in the profile.
8. Click **Save and Close**.

Results:

Users who are assigned the talent pool security profile can access, select, or report on talent pools that are associated with the business units, departments, and job families specified in the security profile.

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 the lists of countries. The predefined country security profile, View All Countries, meets the needs.

However, you can limit the country list available to an HCM data role by creating a country security profile for that role. You can include the countries that are defined in the table FND_TERRITORIES. By default, users with these predefined job and abstract roles see all countries in lists of countries:

- Benefits Administrator
- Benefits Manager
- Benefits Specialist
- Compensation Manager
- Contingent Worker (ORA_PER_CONTINGENT_WORKER_ABSTRACT)
- Employee (ORA_PER_EMPLOYEE_ABSTRACT)
- Human Capital Management Integration Specialist
- Human Resource Specialist (ORA_PER_HUMAN_RESOURCE_SPECIALIST_JOB)
- Line Manager (ORA_PER_LINE_MANAGER_ABSTRACT)

If you include any of these roles in a data role, then users with the data role see all countries. The country security profile that you include in the data role has no effect.

When do I need a job requisition security profile?

By default, users can view job requisitions when they're members of the job requisition hiring team. They can also see the job requisitions that their subordinates can see.

You can define job requisition security profiles and include them in HCM data roles to enable users to view other job requisitions. For example, you can secure access to job requisitions by location or recruiting type.

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

How do I know which 'Organization hierarchy' scope to select for Area of Responsibility?

For person security profile, if you choose Organization hierarchy for department as scope, you get access to people who are working in department present in subbranch of the organization tree, which the signed in user is responsible for.

If you choose Organization hierarchy for legal employer as scope, you get access to people who are working in legal employer present in the subbranch of the organization tree, which the signed in user is responsible for.

For position security profile, if you choose Organization hierarchy for department as scope, you get access to positions from departments present in subbranch of the organization tree, which the signed in user is responsible for.

Alternatively, Organization hierarchy for business unit grants access to positions from business units present in the subbranch of your organization tree, which the signed in user is responsible for.

Why doesn't 'Organization hierarchy for legal employer' appear as an option under Scope of Responsibility for position security profile?

As positions aren't associated with a legal employer, the scope 'Organization hierarchy for legal employer' isn't valid for defining position security access.

19 Using the Security Console

Graphical and Tabular Role Visualizations

On the Roles tab of the Security Console, you can review role hierarchies. You see either a tabular or a graphical view of a role hierarchy, depending on the setting of the Enable default table view option on the Administration tab.

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 column search field 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** icon 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.

Simulate Navigator Menus

You can simulate the Navigator menus 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 roles, for example.

Simulate 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 entry may not appear in the Navigator as the result of configuration, for example.

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

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

View 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.

View 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 creating 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.

Simulate 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.

Review Role Assignments

You can use the Security Console to either view the roles assigned to a user, or to identify the users who have a specific role.

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

View the Roles Assigned to a User

Follow these steps:

1. Open the Security Console.
2. On the Roles tab, 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:

   a. Select the role and right-click.
   b. 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 this view.

Identify Users Who Have a Specific Role

Follow these steps:

1. On the Roles tab of 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, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. 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.

Review Role Hierarchies

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. On the Roles tab of the Security Console, ensure that **Expand Toward** is set to **Privileges**.
2. Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.
3. 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 a column search field 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.

Compare Roles

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.

Compare 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 **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
5. Set **Show** to one of the values shown in this table 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

   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**. You can query by example to filter the results. The comparison is refreshed automatically if you change the **Show** or **Filter Criteria** values.

   > **Tip:** Click **Export to Excel** to save the comparison data to a spreadsheet.

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.

Copy Privileges to the Second Role in the Comparison

You can make some updates to the second role in the comparison without having to edit the role explicitly. That is, you can copy a selected function or data security policy from the first role to the second role when you set:

- **Filter Criteria** to either **Function security policies** or **Data security policies**
- **Show** to **Only in first role**

> **Note:** The second role in the comparison must be a custom role.

To copy a selected policy to the second role, you click **Add to Second Role**.

Compare Users

You can compare users to identify their access permissions and assign the missing permissions as required. This comparison includes both direct and inherited roles. From the results, you can find out if there are any discrepancies in roles.

Users with the following privileges can compare users:

- Create User Account (ASE_CREATE_USER_ACCOUNT_PRIV)
- Edit User Account (ASE_EDIT_USER_ACCOUNT_PRIV)
- View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)
- Delete User Account (ASE_DELETE_USER_ACCOUNT_PRIV)
- Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)
- Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)

On the User Accounts page, you can compare users in two different ways:

- Use the Compare Users button.
- Search for a user and then click Compare Users from the Actions menu of that user.

Follow these steps:

1. On the Security Console, click **Users**.
2. Click **Compare Users**.
3. Search for and select both users one after another.
4. Click **Compare**. All the details of both the users are displayed.

In the comparison results, you can do the following actions:

- Click one of the **Show** options to view the corresponding details in the results.

- Click the Query By Example icon to enter the name of a specific role that you want to see from the search results.

You can then use the Export to Excel option to export the filtered search results.

Role Information on the Analytics Tab

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.

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 column search fields 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.

Analytics for Data Resources

You can review information about data security policies that grant access to a data resource, or about roles and users granted access to that resource.

1. On the Analytics page, click the Database Resources tab.
2. Select the resource that you want to review in the **Data Resource** field.
3. Click **Go**.

   Results are presented in three tables.

Data Security Policies

The Data Security Policies table documents policies that grant access to the selected data resource.

Each row documents a policy, specifying by default:

- The data privileges that it grants.
- The condition that defines how data is selected from the data resource.
- The policy name and description.
- A role that includes the policy.

For any given policy, this table might include multiple rows, one for each role in which the policy is used.

Authorized Roles

The Authorized Roles table documents roles with direct or indirect access to the selected data resource. Any given role might include the following:

- One or more data security policies that grant access to the data resource. The Authorized Roles table includes one row for each policy belonging to the role.
- Inherit access to the data resource from one or more roles in its hierarchy. The Authorized Roles table includes one row for each inheritance.

By default, each row specifies the following:

- The name of the role it documents.
- The name of a subordinate role from which access is inherited, if any. (If the row documents access provided by a data security policy assigned directly to the subject role, this cell is blank.)
- The data privileges granted to the role.
- The condition that defines how data is selected from the data resource.

> **Note:** A role's data security policies and hierarchy might grant access to any number of data resources. However, the Authorized Roles table displays records only of access to the data resource you selected.

Authorized Users

The Authorized Users table documents users who are assigned roles with access to the selected data resource.

By default, each row specifies a user name, a role the user is assigned, the data privileges granted to the user, and the condition that defines how data is selected from the data resource. For any given user, this table might include multiple rows, one for each grant of access by a data security policy belonging to, or inherited by, a role assigned to the user.

Manipulating the Results

In any of these three tables, you can do the following actions:

- Add or remove columns. Select **View - Columns**.
- Search among the results. Select **View - Query by Example** to add a search field on each column in a table.
- Export results to a spreadsheet. Select the **Export to Excel** option available for each table.

20 Creating and Editing Job, Abstract, and Duty Roles

Guidelines for Copying HCM Roles

Copying predefined roles and editing the copies is the recommended approach to creating 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 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.

What Role Copy Does

When you copy a role on the Security Console, the role is copied in accordance with the role-copy options that you specify. Nothing else is updated. For example:

- If the role that you're copying is referenced in an EL expression, then the expression isn't updated to include the new role.
- The new role isn't assigned automatically to users who have the original role.

Related Topics

- Security Console Role-Copy Options
- Copy Job Role and Abstract Role
- Role Preferences
- User and Role Access Audit Report

Security Console Role-Copy Options

When you copy a role on the Security Console, you have the option to either copy top role, or copy top role and inherited roles. This topic explains the effects of each of these options.

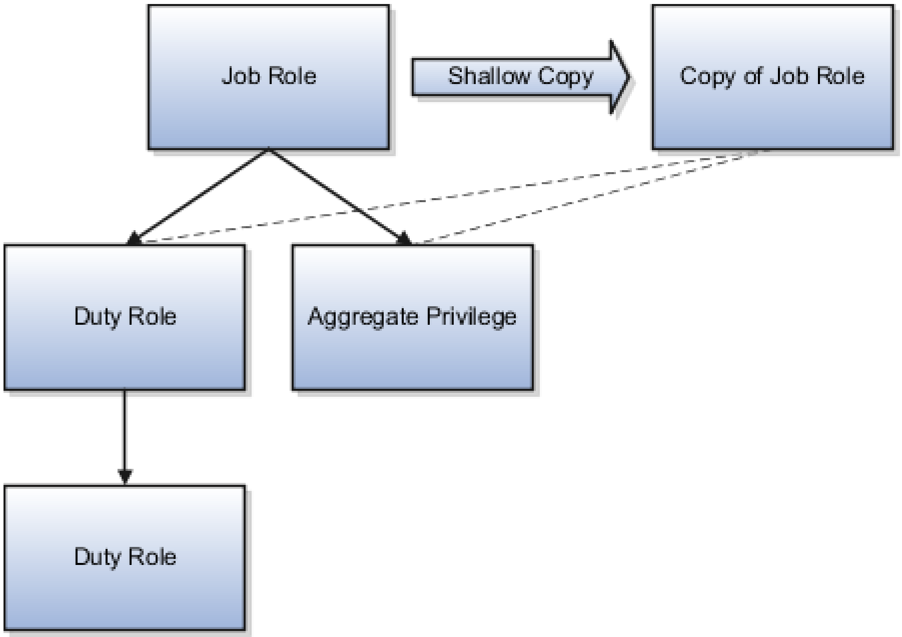
Copy Top Role

If you select the **Copy top role** option, then only the top role from the selected role hierarchy is copied. Memberships are created for the copy in the roles of which the original is a member. That is, the copy of the top role references the inherited role hierarchy of the source role. Any changes made to those inherited roles appear in both the source role and the copy. Therefore, you must take care when you edit the role hierarchy of the copy. You can:

- Add roles directly to the copy without affecting the source role.
- Remove any role from the copy that it inherits directly without affecting the source role. However, if you remove any role that's inherited indirectly by the copy, then any role that inherits the removed role's parent role is affected.
- Add or remove function and data security privileges that are granted directly to the copy of the top role.

If you copy a custom role and edit any inherited role, then the changes affect any role that inherits the edited role.

The option of copying the top role is referred to as a shallow copy. This figure summarizes the effects of a shallow copy. It shows that the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.



You're recommended to create a shallow copy unless you must make changes that could affect other roles or that you couldn't make to predefined roles. 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.

> **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.

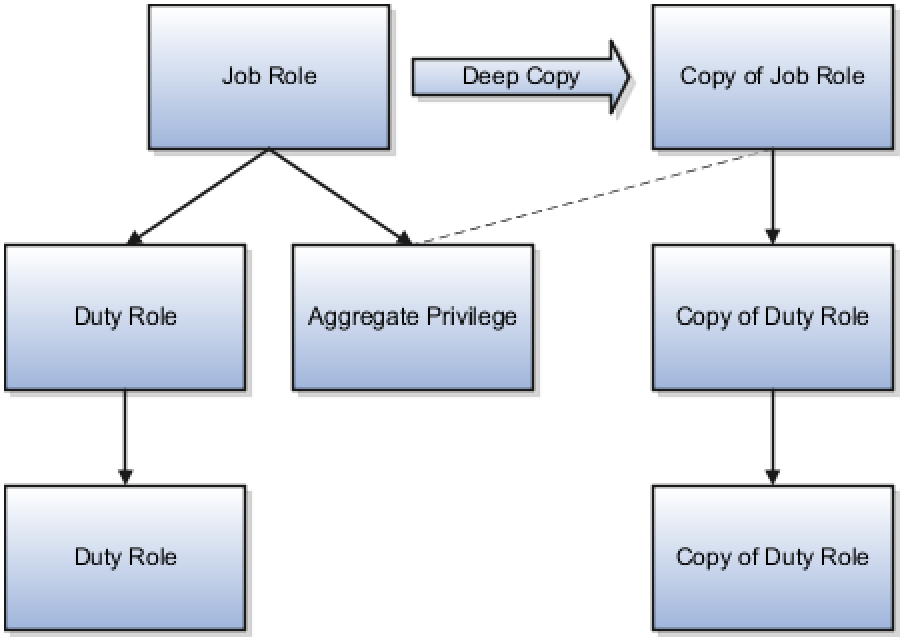
Copy Top Role and Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. These rules apply:

- Inherited aggregate privileges and middleware roles are never copied. Instead, membership is added to each aggregate privilege, or middleware role, for the copy of the source 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 new role.

When inherited duty roles are copied, custom duty roles are created. Therefore, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copies of those roles. For example, if those duty roles are predefined and are updated during upgrade, then you may have to update your copies manually after upgrade. This option is referred to as a deep copy.

This figure shows the effects of a deep copy. In this example, copies of the inherited duty roles with the same name don't already exist. Therefore, the inherited duty roles are copied when you copy the top role. Aggregate privileges are referenced from the new role.



Related Topics

- Guidelines for Copying HCM Roles
- Copy Job Role and Abstract Role

Guidelines for Copying Abstract Roles

Roles with assigned security profiles contain data security policies that are generated from the assigned security profiles.

When you copy such a role, you copy all of its data security policies, including those that were generated from the assigned security profiles. These data security policies can be difficult to remove successfully from the role copy on the Security Console. Therefore, to avoid copying unwanted data security policies, you're recommended to revoke security profiles from abstract roles before you copy them. Reassign the security profiles to the abstract role when the copy is complete.

> **Tip:** If you have already made a copy of a predefined abstract role with assigned security profiles, then you can remove the copied data security policies as follows:
>
> 1. Edit your custom role.
> 2. On the Data Security Policies page, filter by policy names beginning with the prefix **ORA_**. These policies were generated from security profiles assigned to the predefined abstract role that you copied.
> 3. Remove all policies beginning with **ORA_** in the filtered list.
>
> Any remaining data security policies are either predefined and should not be removed or generated from security profiles assigned to your custom role.

Related Topics

- Security Console Role-Copy Options

Copy Job Role and Abstract Role

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. You must have the IT Security Manager job role or privileges for this task.

The following video shows how you can copy a predefined abstract role:

Watch video

Copy 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:** If you prefer, 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**, **Description**, and **Enable Role for Access from All IP Addresses** values, as appropriate. **Enable Role for Access from All IP Addresses** appears only if location-based access is enabled.

   > **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 on the Copy Role: Basic Information page.

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 Status subtab of the Security Console Administration tab. When the status is **Complete**, you can edit the copied role.

   If you prefer, you can visit the intermediate train stops after the Copy Role: Basic Information page and edit your copy of the role before you save it.

Related Topics

- Security Console Role-Copy Options
- Guidelines for Copying HCM Roles
- Edit Job Role and Abstract Role

Edit Job Role and Abstract Role

You can create a role by copying a predefined job role or abstract role and editing the copy. You must have the IT Security Manager job role or privileges to perform this task.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see the topic *Guidance for Assigning Predefined Roles*.

Edit 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. If location-based access is enabled, then you can also manage the **Enable Role for Access from All IP Addresses** option.
4. Click **Next**.

Manage Functional Security Privileges

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. 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.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the Edit Role: Role Hierarchy page, if appropriate.

   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.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Manage Data Security Policies

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

Add and Remove 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.

> **Note:** The role that you're removing must be inherited directly by the role that you're editing. If the role is inherited indirectly, then you must edit its parent role.

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**.

Provision the Role to Users

To provision the role to users, you must create a role mapping. Don't provision the role to users on the Security Console.

Review 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.

Related Topics

- Copy Job Role and Abstract Role

Manage Role Definitions Using CSV File Packages

As an alternative to editing role definitions using the Security Console, you can edit them using CSV File Packages.

This method is useful if you want to make mass updates to a custom job or abstract role, and you know the exact names of the roles and privileges you want to add or remove from your custom role. You cannot add or remove data security policies using this approach.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see the topic *Guidelines for Configuring Security*.

Export Custom Role Definition to a CSV File Package

Follow these steps:

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. Select the **Workforce Deployment** offering.
3. Select the **Users and Security** functional area.
4. Select the **Manage Job Roles** task and choose the **Export to CSV File** > **Create New** action.
5. Add your custom job or abstract role to the **Functional Security Custom Roles: Scope**.
6. Click **Submit** to initiate the export of your custom role definition.
7. Choose the **Export to CSV File** > **View All** action to monitor the progress of the export.
8. When the export has completed, select **Download** > **CSV File Package** from the **Actions** menu. This will download a .zip file to your desktop.

Modify the CSV File Package

Follow these steps:

1. Extract the .zip file and view the contents. There will be four files.
   - ASM_SETUP_CSV_METADATA.xml - Defines the structure of the CSV files
   - ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLES.csv - Contains basic information about each of the exported roles
   - ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLE_HIERARCHY.csv - Contains the role hierarchy memberships for the exported roles
   - ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLE_PRIVILEGE_MEMBERSHIP.csv - Contains the function security privilege grants for the exported roles
     You don't need to make any changes to ASM_SETUP_CSV_METADATA.xml.
     To add aggregate privileges or duty roles to your custom role hierarchy, add rows to the ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLE_HIERARCHY.csv file and enter ADD in the "AddOrRemoveRoleMembership" column. Use the aggregate privilege or role codes, not the display names.
     To remove aggregate privileges or duty roles from your custom role hierarchy, update the rows containing the aggregate privilege or role codes you want to remove in the ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLE_HIERARCHY.csv file and enter REMOVE in the "AddOrRemoveRoleMembership" column.
     Make similar changes in the ORA_ASE_FUNCTIONAL_SECURITY_CUSTOM_ROLE_PRIVILEGE_MEMBERSHIP.csv to add and remove function security privilege grants from your custom role.
     If you remove rows from either of these CSV files, no changes will be made to your custom role with respect to the rows that you remove.
2. When you have finished updating the CSV files, compress the three CSV files and the ASM_SETUP_CSV_METADATA.xml file into a .zip file. This is the CSV File Package that you will import in the next section.

Import the CSV File Package

Follow these steps to import the CSV File Package and upload the changes to your custom role definition:

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. Select the **Workforce Deployment** offering.
3. Select the **Users and Security** functional area.
4. Select the **Manage Job Roles** task and choose the **Import from CSV File** > **Create New** action.
5. Choose the .zip file you created earlier when prompted for a CSV File Package.
6. Click **Submit** to initiate the import of your CSV File Package.
7. Choose the **Import from CSV File** > **View All** action to monitor the progress of the import.
8. When the import has completed, review your custom role in the Security Console to verify that the changes have been applied.

Regenerate Roles

If you have made changes to the role hierarchy of a custom job role, regenerate any data roles that inherit this job role.

If you have made changes to the role hierarchy of an abstract role, regenerate the abstract role.

Related Topics

- Regenerate Roles
- Managing Role Definitions Using CSV File Packages

Create Job Role and Abstract Role from Scratch

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

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see the topic *Guidelines for Configuring Security*.

Enter 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 **XYZ HR Business Partner**.
3. Complete the **Role Code** field. For example, enter **XYZ_HR_BUSINESS_PARTNER_JOB**.
   Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**. Default prefixes for role codes and role names can be specified on the Roles subtab of the Security Console's Administration tab. These are used when copying roles. It’s a good practice to use the same prefixes when defining job and abstract roles from scratch as when copying roles. This ensures that your custom roles follow the same naming pattern, whether they have been copied from other roles or created from scratch.
4. In the **Role Category** field, select either **HCM - Abstract Roles** or **HCM - Job Roles**, as appropriate.

   > **Note:** Be sure to select the **HCM - Job Roles** category when creating job roles. Otherwise, your job roles don't appear in the list of available job roles when you create an HCM data role.

5. If you're using location-based access, then you see the **Enable Role for Access from All IP Addresses** option. If you select this option, then users who have the role can access the tasks that the role secures from any IP address.
6. Click **Next**.

Add 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 Privileges tab of 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.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the **Create Role: Role Hierarchy** page, if appropriate.

   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**.

You're recommended to include the following function security privileges in all HCM custom job and abstract roles:

- Approve Transactions - PER_APPROVE_TRANSACTIONS_PRIV
- View Notification Details - PER_VIEW_NOTIFICATION_DETAILS_PRIV
- Access HCM Common Components - HRC_ACCESS_HCM_COMMON_COMPONENTS_PRIV

If your custom job and abstract role are granted access to any of the responsive user experience pages, you might need to also add function security privileges that grant access to Lists of Values. For more information, see the topic *Privileges Roles Securing Lists of Values in Responsive User Experience Pages*.

> **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.

Create Data Security Policies

Make no entries on the **Create Role: Data Security Policies** page.

Build 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**.

If your custom job and abstract role are granted access to any of the responsive user experience pages, you might need to also add aggregate privileges that grant access to Lists of Values. For more information, see the topic *Privileges and Roles Securing Lists of Values in Responsive User Experience Pages*.

Provision the Role

To provision the role to users, you must create a role mapping when the role exists. Don't provision the role to users on the Security Console.

Review 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.

Copy and Edit Duty Roles

You can copy a duty role and edit the copy to create a duty role. Copying duty roles is the recommended way of creating duty roles. You must have the IT Security Manager job role or privileges to perform these tasks.

Copy 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:** If you prefer, 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 on the Copy Role: Basic Information page.

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 Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Edit 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**.

Manage Functional Security Policies

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. 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**.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the Edit Role: Role Hierarchy page, if appropriate.

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.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Manage Data Security Policies

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

Add and Remove 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**.

Review 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.

Related Topics

- Guidelines for Copying HCM Roles
- Security Console Role-Copy Options

21 Regenerating Roles

Regenerate Roles

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.

Regenerate Multiple Roles

To regenerate multiple roles at once, you use the **Regenerate Data Security Grants** process.

Regenerate Roles Individually

To regenerate a single data or abstract role, you can use the **Regenerate Data Security Grants** 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.

Related Topics

- Implementing Assignment-Level Security in HCM (Doc ID 2700661.1)

Run the Regenerate Data Security Grants Process

You must regenerate an HCM data role if changes are made to the data security policies of its inherited job role. 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 Regenerate Data Security Grants process. This topic describes how to run this process.

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.

Run Regenerate Data Security Grants Process

Follow these steps.

1. Sign in with the following roles or privileges:
   - IT Security Manager
   - Human Resource Specialist
   - Human Capital Management Application Administrator
2. Open the Scheduled Processes work area.
3. In the Scheduled Processes work area, click **Schedule New Process**.
4. In the Schedule New Process dialog box, search for and select the **Regenerate Data Security Grants** process.
5. Click **OK**.
6. In the Process Details dialog box, set the **Mode** value to identify the types of roles to process. 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.
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.

7. If you are regenerating an individual role, select the role.
8. Click **Submit** .

Related Topics

- Regenerate Roles

Regenerate Data Security Profiles and Grants Job Set

After upgrade, you must regenerate HCM data roles that inherit updated job roles. You must also regenerate updated abstract roles to which security profiles are assigned. The job and abstract roles might be predefined or custom.

We recommend regenerating your security profiles to uptake changes that Oracle might deliver as part of the upgrade. The **Regenerate Data Security Profiles and Grants** job set streamlines the regeneration of HCM data roles, abstract roles, and security profiles.

> **Note:** The Regenerate Data Security Profiles and Grants job set is run automatically for you at quarterly upgrade. However, it is essential that you verify that the job set is successfully completed. We don't recommend scheduling this job set on a recurring basis. We expect that this job set process will complete by the time your updated environment is released back to you; however, it might still be in Running status. You need to wait until the status is Succeeded or Completed before starting any regression testing. The process might take longer for larger organizations.

Verify Successful Completion of the Regenerate Data Security Profiles and Grants Job Set

Follow these steps:

1. Sign in as an IT Security Manager user, or another user with IT Security Manager access.
2. Open the Scheduled Processes work area.
3. In the Scheduled Processes work area, search for the **Regenerate Data Security Profiles and Grants** job set process and verify that the status is either **Succeeded** or **Completed**.
4. If your job set does not complete successfully, try to rerun it manually.

Manually Run the Regenerate Data Security Profiles and Grants Job Set

Follow these steps:

1. Sign in as an IT Security Manager user, or another user with IT Security Manager access.
2. Open the Scheduled Processes work area.
3. In the Scheduled Processes work area, click **Schedule New Process** and select **Job Set** in the dialog box.
4. Select **Regenerate Data Security Profiles and Grants** job set and click **OK**.

You might need to manually run the job set if you're switching between assignment and person-based security. For more information on assignment-level security, see Implementing Assignment-Level Security in HCM (2700661.1).

Related Topics

- Implementing Assignment-Level Security in HCM (Doc ID 2700661.1)

22 Securing Access to Value Sets

Enable Security for Value Sets

A value set is a group of valid values that you assign to a flexfield segment. When you enter a value for that flexfield segment, the value is validated against the value set.

Use the **Manage Value Sets for Global Human Resources** task in the Setup and Maintenance work area to manage value sets. This topic describes how to enable security for value sets so that they're available to specific users or processes only. It also summarizes how secured access to value sets is implemented.

Enable Security

When you create a value set where the **Validation Type** is **Independent**, **Dependent**, **Subset**, or **Table**, then you can enable security for that value set. When you're enabling security on table-validated value sets, the value set must be based on a single table or view. On the Create Value Set page, you:

1. Select the **Security enabled** option. This selection enables data security policies to control user access to the values in the value set.
2. Enter a name in the **Data Security Resource Name** field. This value identifies the value set that you want to secure. Typically, this value is the same as the **Value Set Code**.

   > **Tip:** You need the **Data Security Resource Name** value later when securing access to the value set on the Security Console.

Define Data Security Policies to Secure Access to Value Sets

When security is enabled for a value set, you can create a data security policy for the data set. You grant the data security policy to a predefined duty role. The role that you use for this purpose is Custom Data Security Policies for Application Identities (ORA_HRC_APPLICATION_IDENTITY_CUSTOM_DSPS). These predefined APPIDs inherit this duty role:

- FUSION_APPS_HCM_ESS_APPID
- FUSION_APPS_HCM_ESS_LOADER_APPID
- FUSION_APPS_HCM_SOA_APPID
- FUSION_APPS_OBIA_BIEE_APPID

> **Note:** An APPID is a predefined user to which specific types of access, such as permission to run batch processes, is granted.

Processes that require access to secured value sets can then access those value sets. For example, access to value sets in the Cost Allocation Key Flexfield for payroll processes is secured in this way.

Related Topics

- Secure Access to Value Sets

Secure Access to Value Sets

This topic shows how to grant data security policies to the predefined Custom Data Security Policies for Application Identities duty role. These data security policies secure access to value sets.

Follow these steps:

1. Sign in with the IT Security Manager role or privileges.
2. Select **Navigator** > **Tools** > **Security Console**.
3. On the Roles tab of the Security Console, search for the Custom Data Security Policies for Application Identities (ORA_HRC_APPLICATION_IDENTITY_CUSTOM_DSPS) duty role.
4. Select the role in the search results.
5. From the **Actions** menu for the role, select **Edit Role**.

   > **Tip:** You can add data security policies to a predefined role without first having to create a copy of the role. This type of modification survives upgrade.

6. On the Basic Information page, click the **Data Security Policies** train stop.
7. On the Data Security Policies page, click **Create Data Security Policy**.
8. In the Create Data Security Policy dialog box:

   a. Enter a policy name, for example, **Access Secured Value Sets VISION_SECURED_VALUE_SET**.
   b. In the **Database Resource** field, search for and select the name that you defined for your value set.

      > **Tip:** You created this value on the Create Value Set page after selecting **Security enabled** for the value set.

   c. Enter a start date. Use a value on or before today's date so that you can test user access to the value set.
   d. Set **Data Set** to **All values**.
   e. Set **Actions** to **Read**.
   f. Click **OK**.
9. Repeat from step 7 for additional value sets.
10. On the Data Security Policies page, click the **Summary and Impact Report** train stop.
11. Review the summary of your changes.
12. Click **Save and Close**.
13. Click **OK** to close the confirmation dialog box.

Processes running with any of the APPIDs that inherit Custom Data Security Policies for Application Identities now have secured access to relevant value sets.

Related Topics

- Enable Security for Value Sets

23 Securing Content Sections in Person Profiles

How You Secure Content Sections in Person Profiles

Sensitive data for a worker appears in content sections in person profiles. To give users an appropriate level of access to person profile contents, you can secure this information at the content section level.

For example, a person profile can contain information about competencies, performance ratings, job criticality, risk of loss, degrees, and so on. This topic:

- Introduces content types and content sections
- Describes the task that manages content-section access for selected roles
- Explains how data security policies are constructed to secure access to custom content types
- Describes regeneration of the affected data and abstract roles

Content Types and Content Sections

Content types are the skills, qualities, and qualifications that you track in talent profiles. You select content types from the content library to create content sections for the profile type. You can secure access to content sections in person profiles only. The content types can be either predefined or custom but must be associated with the person profile type.

Manage Profile Content Section Access

Use the **Manage Profile Content Section Access** task in the Setup and Maintenance work area to secure access to content sections in person profiles. You must have the IT Security Manager job role or privileges to perform this task. For a selected content section, you can:

- Identify the predefined or custom job roles and abstract roles that can access the content section in person profiles.
- Specify the level of access for each role. This table describes the levels.

Access Level	Description
View	Users can view content-section data.
Edit	Users can edit content-section data. This access includes View and Report access.
Report	Users can include content-section data in Oracle Business Intelligence Publisher reports.

Data Security Policies

When you map a predefined content type to a role, a predefined data security privilege is granted to the role automatically. When you map a custom content type to a role, a data security privilege is both generated and granted to the role automatically. For example, you could map the custom Leadership content type to the predefined Employee abstract role and set the access level to **Edit**. This table shows the resulting data security policy. The data security privilege shown in this data security policy would be generated and granted to the role.

Data Security Policy	Data Resource	Data Security Privilege	Condition
ORA_PER_EMPLOYEE_ABSTRACT, Grant on Profile Content Type LEADERSHIP	Person Detail	Manage Leadership Content Type	HCM:PER:PER_ALL_PEOPLE_F:View Own Record

These rules apply to the data security policy:

- The policy name is in the form: `role code, Grant on Profile Content Type content type code`. The policy description is the same as the policy name.
- The data resource is Person Detail.
- The data security privileges are in the form: `Manage | Report | View | content type name Content Type`
- The condition, which controls access to specific instances of person records, identifies the relevant person security profile.

Note: Don't create custom data security policies on the Security Console to manage profile content section access. Always use the **Manage Profile Content Section Access** task.

Regeneration of Data and Abstract Roles

After saving your changes on the Manage Profile Content Section Access page, you must regenerate:

- Data roles that inherit any of the job roles to which you mapped a content section
- Abstract roles to which you mapped a content section and to which security profiles are assigned

Regenerating roles updates their data security permissions. If you don't regenerate relevant roles, then users can't access content sections in person profiles.

Note: If you plan to copy abstract or job roles to which security profiles are assigned, then revoke the security profiles before you perform the copy. This precaution ensures that any data security policies, including those generated when you map content sections to a role, aren't copied.

Restrictions

Content sections in person profiles are unsecured when person profiles are included in:

- Best-fit analyses
- Profile comparisons
- Oracle Transactional Business Intelligence reports

Related Topics

- Secure Content Sections in Person Profiles
- Regenerate Roles

Secure Content Sections in Person Profiles

You can enable a job role or abstract role to access selected content sections in person profiles. You can also specify the level of access for each role. This topic describes how to perform this task.

You must have the IT Security Manager job role or privileges to perform this task. Sign in and follow these steps:

1. In the Setup and Maintenance work area, use the **Manage Profile Content Section Access** task.
2. In the Content Sections section of the Manage Profile Content Section Access page, select a content section.

   The Roles section is updated automatically for the selected content section. It shows any roles that already have access to the content section and their access level. You can change the access level, if appropriate.
3. To map the content section to a job or abstract role:

   a. In the Roles section of the page, click **Add**.
   b. Search for and select the role.
   c. Select any combination of **View**, **Edit**, and **Report** to set the access for the role. When you select **Edit**, **View** and **Report** are selected automatically.

   Repeat this step for additional roles.
4. To remove a role, select it and click **Remove**.
5. Save your changes.
6. Repeat from step 2 for additional content sections.

> **Note:** You must regenerate:
>
> - Data roles that inherit any of the job roles to which you mapped a content section
> - Abstract roles to which you mapped a content section and to which security profiles are assigned

Related Topics

- How You Secure Content Sections in Person Profiles
- Regenerate Roles

24 Securing Access to Succession Plans, Incumbents, and Candidates

Overview of How to Secure Access to Succession Plans, Incumbents, and Candidates

This topic provides an overview of the ways in which you can configure user access to succession plans, incumbents, and candidates.

Providing Access to All Succession Plans in the Succession Plans Work Area

No predefined job role enables any user to manage all succession plans in the Succession Plans work area. To give selected users this access, you can create a super user job role and provision the job role directly to those users. The job role is granted custom data security policies that provide access to all succession plans including private succession plans.

You can also enable users with this super user job role to access Oracle Transactional Business Intelligence (OTBI) subject areas for all succession plans. You can either edit your custom job role to add OTBI access or provide a separate job role that has OTBI access. By creating one role with OTBI access and one without, you can provide selective access to OTBI subject areas for succession management.

Configuring Access to Lists of Succession Plan Incumbents and Candidates

Human resource (HR) specialists and line managers select incumbents and candidates from lists of workers secured by the person security profiles assigned to their roles. However, you may want to present different lists of workers to HR specialists and line managers when they're selecting incumbents and candidates. For example, you may want to restrict the lists in some way or include workers who would not otherwise appear. To achieve this flexible access, you can replace the predefined data security policies that secure access to these lists with custom data security policies. As the incumbent and candidate lists are secured separately, you can specify different conditions for each list. For example, you could specify that:

- The list of incumbents includes only workers in a specific location.
- The list of candidates includes only workers in the legal employer for which the HR specialist has the human resources representative responsibility.

Related Topics

- Create a Succession Plans Super User Job Role
- Configure Access to Lists of Incumbents and Candidates

Create a Succession Plans Super User Job Role

In this example, you learn how to create a job role that provides access to all succession plans in the Succession Plans work area.

The following table summarizes key decisions for this scenario.

Decisions to Consider	In This Example
What's the name of the job role?	Succession Plans Super User Job
What's the code of the job role?	SUCCESSION_PLANS_SUPER_USER_JOB
What are the names of the data security policies?	• Succession Plans Custom Policy • Succession Candidate Custom Policy • Succession Person Detail Custom Policy
What's the enterprise suffix for copied roles?	Custom
Is there an enterprise prefix for copied roles?	No
What's the name of the role mapping?	Access All Succession Plans
How do users acquire the role?	Users with the human resources representative responsibility can provision the role to other users.

Summary of the Tasks

Enable access to all succession plans in the Succession Plans work area by:

1. Copying the predefined Succession Plan Management duty role and editing the copy
2. Creating a job role
3. Granting data security policies to the job role
4. Creating a role hierarchy for the job role
5. Creating a role mapping
6. Optionally, editing the job role to enable access to Oracle Transactional Business Intelligence (OTBI) subject areas for Succession Management

Copy the Succession Plan Management Duty Role

You copy the predefined Succession Plan Management duty role and edit it to remove the existing data security policy.

1. Sign in with the IT Security Manager job role or privileges and select **Navigator** > **Tools** > **Security Console**.

2. On the Roles tab of the Security Console, search for the predefined **Succession Plan Management** (ORA_HRM_SUCCESSION_PLAN_DUTY) duty role.
3. In the search results, select **Copy Role** on the role's **Actions** menu.
4. In the Copy Options dialog box, select **Copy top role** and click **Copy Role**.

   On the Copy Role: Basic information page, the name of the copied role is Succession Plan Management Custom (HRM_SUCCESSION_PLAN_DUTY_CUSTOM).
5. Click the **Data Security Policies** train stop.

   On the Data Security Policies page, the Grant on Succession Plan Detail policy is listed.
6. On the **Actions** menu for the data security policy, click **Remove Data Security Policy**.
7. In the Warning dialog box, click **Yes**.
8. Click the **Summary and Impact Report** train stop.
9. On the Summary and Impact Report page, click **Submit and Close** to create the duty role.
10. Click **OK** to close the Confirmation dialog box.

Create a Job Role

You create the Succession Plans Super User Job role.

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role name **Succession Plans Super User Job**.
3. Enter the role code **SUCCESSION_PLANS_SUPER_USER_JOB**.
4. In the **Role Category** field, select **HCM - Job Roles**.
5. Click the **Data Security Policies** train stop.

Grant Data Security Policies to the Job Role

You create three data security policies for the Succession Plans Super User Job role.

1. On the Data Security Policies page, click **Create Data Security Policy** to open the Create Data Security Policy dialog box.
2. In the Create Data Security Policy dialog box, enter the policy name **Succession Plans Custom Policy**.
3. Search for and select the database resource **Succession Plan Detail** (HRM_PLANS).
4. Select **All values** in the **Data Set** field.
5. Select these values in the **Actions** field:
   - Add Worker to Succession Plan
   - Create Succession Plan for Worker
   - Manage Succession Plan
   - View Succession Plan
6. Click **OK** to close the Create Data Security Policy dialog box.
7. Repeat from step 1 to create two further data security policies. Complete the fields as shown in this table.

Policy Name	Database Resource	Data Set	Actions
Succession Candidate Custom Policy	Succession Plan Candidate (HRM_PLAN_CANDIDATES)	All values	◦ Manage Succession Plan Candidate ◦ View Succession Plan Candidate

Policy Name	Database Resource	Data Set	Actions
Succession Person Detail Custom Policy	Person Detail (PER_ALL_PEOPLE_F)	All values	◦ Add Worker to Succession Plan ◦ Create Succession Plan for Worker ◦ View Succession Plan

You now see the three data security policies listed on the Data Security Policies page.

Define the Role Hierarchy for the Job Role

You add the Create Succession Plan for Worker aggregate privilege and the Succession Plan Management Custom duty role to the Succession Plans Super User Job role hierarchy.

1. Click the **Role Hierarchy** train stop.
2. On the Role Hierarchy page, click **Add Role**.
3. In the Add Role Membership dialog box, search for the **Create Succession Plan for Worker** (ORA_HRM_SUCCESSION_PLAN_CREATE_DUTY) aggregate privilege.
4. Select the aggregate privilege in the search results and click **Add Role Membership**.
5. Repeat from step 3 to add the Succession Plan Management Custom duty role.
6. Close the Add Role Membership dialog box.
7. Click the **Summary and Impact Report** train stop.
8. Click **Save and Close**.
9. Click **OK** to close the Confirmation dialog box.

Create a Role Mapping

You create a role mapping to enable the Succession Plans Super User Job role to be provisioned to users.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Workforce Deployment
   - Functional Area: Users and Security
   - Task: Manage Role Provisioning Rules
2. On the Manage Role Mappings page, click the **Create** icon in the Search Results section.
3. In the **Mapping Name** field on the Create Role Mapping page, enter **Access All Succession Plans**.
4. Complete the fields in the Conditions section as shown in this table.

Field	Value
HR Assignment Status	Active
Responsibility Type	Human resources representative

5. In the Associated Roles section, click the **Add Row** icon.
6. In the **Role Name** field, search for and select **Succession Plans Super User Job**.

7. Select the **Requestable** option and deselect the **Autoprovision** option.
8. Click **Save and Close**.

   Users with the human resources representative responsibility can now provision the Succession Plans Super User Job role to other users. A user who has the role can manage all succession plans in the Succession Plans work area with the following exceptions:

   - A user who is also the Candidate Manager for a plan can edit only the plan's candidate list.
   - A user who is also the Viewer of a plan can view the plan but not edit it.

Enable Access to OTBI Subject Areas

To enable users who have the Succession Plans Super User Job role to access OTBI subject areas for Succession Management, you edit two of the job role's data security policies and add a role to the role hierarchy.

1. Sign in with the IT Security Manager job role or privileges and select **Navigator** > **Tools** > **Security Console**.
2. On the Roles tab of the Security Console, search for the **Succession Plans Super User Job** role.
3. In the search results, select **Edit Role** on the role's **Actions** menu.
4. Click the **Data Security Policies** train stop.
5. On the **Actions** menu for the Succession Plans Custom Policy data security policy, select **Edit Data Security Policy**.
6. In the Edit Data Security Policy dialog box, select **Report Succession Plan** in the **Actions** field.
7. On the **Actions** menu for the Succession Person Detail Custom Policy data security policy, select **Edit Data Security Policy**.
8. In the Edit Data Security Policy dialog box, select **Report on Succession Plan Candidacy**, and **Report on Succession Plan Incumbent**, in the **Actions** field.
9. Click **OK** to close the Edit Data Security Policy dialog box.
10. Click **Create Data Security Policy** to open the Create Data Security Policy dialog box.
11. In the Create Data Security Policy dialog box, complete the fields as shown in this table:

Policy Name	Database Resource	Data Set	Actions
Succession Talent Profile Custom Policy	Talent Profile for Table HRT_PROFILES_B	All Values	Report Talent Profile

12. Click **OK** to close the Create Data Security Policy dialog box.
13. Click the **Role Hierarchy** train stop.
14. Click **Add Role**.
15. In the Add Role Membership dialog box, search for and select the predefined **Succession Management Transaction Analysis Duty** (FBI_SUCCESSION_MANAGEMENT_TRANSACTION_ANALYSIS_DUTY) role.
16. Click **Add Role Membership**.
17. Close the Add Role Membership dialog box.
18. Click the **Summary and Impact Report** train stop.
19. Click **Save and Close**.

    Any user who has the Succession Management Super User Job role can now access OTBI subject areas for Succession Management.

Related Topics

- Overview of How to Secure Access to Succession Plans, Incumbents, and Candidates

Configure Access to Lists of Incumbents and Candidates

In this example, you learn how to create an HCM data role that provides access to restricted lists of succession plan incumbents and candidates. Human resource (HR) specialists select incumbents and candidates for succession plans from lists of workers.

By default, the workers who appear in those lists are defined by the person security profile assigned to the HR specialist's data role. You may want to vary this access. For example, you may want to present lists of incumbents and candidates that are restricted in some way.

The following table summarizes key decisions for this scenario.

Decisions to Consider	In This Example
What's the name of the HCM data role?	HR Specialist - Restricted Incumbents and Candidates
What are the name and display name of the database resource condition for incumbents?	Incumbent List and Incumbent List Securing Condition
What are the name and display name of the database resource condition for candidates?	Candidate List and Candidate List Securing Condition
How will the database resource conditions be specified?	SQL predicate
Which workers should appear in the lists of incumbents and candidates for HR specialists?	Employees in the department for which the HR specialist has the human resources representative responsibility
What's the name of the data security policy for incumbents?	Restricted Access to Incumbents Policy
What's the name of the data security policy for candidates?	Restricted Access to Candidates Policy

Summary of the Tasks

Enable access to restricted lists of incumbents and candidates by:

1. Creating an HCM data role
2. Creating two database resource conditions
3. Editing the HCM data role to end date existing data security policies

4. Creating replacement data security policies for the HCM data role that reference the new database resource conditions

Create the HCM Data Role

You create an HCM data role with view-all access.

1. Sign in with the IT Security Manager role or privileges.
2. In the Setup and Maintenance work area, go to the following:
    - Offering: Workforce Development
    - Functional Area: Users and Security
    - Task: Assign Security Profiles to Role
3. On 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	HR Specialist - Restricted Incumbents and Candidates
Job Role	Human Resource Specialist

5. Click **Next**.
6. On the Create Role: Security Criteria page, select the security profiles shown in this table.

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)	View All Workers
Person Security Profile (Public Person)	View All People
Document Type Security Profile	View All Document Types
Payroll Security Profile	View All Payrolls

Field	Value
Flow Pattern Security Profile	View All Flows

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

Create Database Resource Conditions

You create two data base resource conditions that you will include in data security policies.

1. Select **Navigator** > **Tools** > **Security Console**.
2. On the Security Console, click the Administration tab.
3. On the General subtab, click **Manage Database Resources**.
4. On the Manage Database Resources and Policies page, enter **PER_ALL_PEOPLE_F** in the **Object Name** field and click **Search**.
5. In the Search Results section, click the **Edit** icon.
6. On the Edit Data Security: PER_ALL_PEOPLE_F page, click the Condition tab.
7. On the Condition tab, click the **Create** icon.
8. In the Create Database Resource Condition dialog box, complete the fields as shown in this table.

Field	Value
Name	Incumbent List
Display Name	Incumbent List Securing Condition
Condition Type	SQL predicate

In the **SQL Predicate** field, enter the following statement:

```
EXISTS(SELECT 1 FROM PER_ALL_ASSIGNMENTS_M ASG,PER_PERIODS_OF_SERVICE PS,PER_ASG_RESPONSIBILITIES RES
 WHERE ASG.ASSIGNMENT_TYPE IN('E')
AND ASG.EFFECTIVE_LATEST_CHANGE='Y' AND SYSDATE BETWEEN ASG.EFFECTIVE_START_DATE AND
 ASG.EFFECTIVE_END_DATE AND PS.PERIOD_OF_SERVICE_ID=ASG.PERIOD_OF_SERVICE_ID
AND (ASG.ASSIGNMENT_STATUS_TYPE IN ('ACTIVE','SUSPENDED') OR (ASG.ASSIGNMENT_STATUS_TYPE IN ('INACTIVE')
 AND NOT EXISTS
SELECT 1 FROM PER_ALL_ASSIGNMENTS_M EXASG WHERE EXASG.ASSIGNMENT_TYPE IN('E','C','N','P') AND
 EXASG.EFFECTIVE_LATEST_CHANGE = 'Y'
AND EXASG.PERSON_ID = ASG.PERSON_ID AND SYSDATE BETWEEN LEAST(SYSDATE,EXASG.EFFECTIVE_START_DATE) AND
 EXASG.EFFECTIVE_END_DATE AND EXASG.ASSIGNMENT_STATUS_TYPE IN
('ACTIVE','SUSPENDED')) AND PS.ACTUAL_TERMINATION_DATE = (SELECT MAX(ALLPS.ACTUAL_TERMINATION_DATE) FROM
 PER_PERIODS_OF_SERVICE ALLPS WHERE
ALLPS.PERSON_ID = ASG.PERSON_ID AND ALLPS.ACTUAL_TERMINATION_DATE IS NOT NULL))) AND SYSDATE BETWEEN
 RES.START_DATE AND NVL(RES.END_DATE,SYSDATE)
AND ASG.PERSON_ID=&TABLE_ALIAS.PERSON_ID AND RES.PERSON_ID=(SELECT
 NVL(HRC_SESSION_UTIL.GET_USER_PERSONID,-1) FROM DUAL) AND
RES.RESPONSIBILITY_TYPE='HR_REP' AND ASG.ORGANIZATION_ID=RES.ORGANIZATION_ID AND ((SELECT
 NVL(HRC_SESSION_UTIL.GET_USER_PERSONID,-1)
FROM DUAL)<>&TABLE_ALIAS.PERSON_ID)))
```

> **Tip:** To generate a SQL predicate that you can use or edit, create a person security profile with the required conditions. Copy the SQL predicate from the SQL Predicate for Person Access tab on the Create Person Security Profile: Preview page.

9. Click **Save**.
10. Repeat steps 7 through 9 for the candidate condition using the values shown in this table and the same SQL predicate.

Field	Value
Name	Candidate List
Display Name	Candidate List Securing Condition
Condition Type	SQL predicate

End Date Data Security Policies Granted to the HCM Data Role

You edit the HCM data role to end date the existing data security policies.

1. Click the Roles tab on the Security Console.
2. Search for and select the HR Specialist - Restricted Incumbents and Candidates data role.
3. In the search results, select **Edit Role** on the role's **Actions** menu.
4. On the Basic Information page, click the **Data Security Policies** train stop.
5. In the **Privilege** search field, enter **Add Worker to Succession Plan** and press **Enter**.
6. In the row containing the specified privilege for the Person Detail data resource, select **Edit Data Security Policy** on the **Actions** menu.
7. In the Edit Data Security Policy dialog box, enter today's date in the **End Date** field.
8. Click **OK** to close the Edit Data Security Policy dialog box.
9. Repeat from step 5 for the Create Succession Plan for Worker privilege.

   Remain on the Data Security Policies page.

Create Data Security Policies

You create two data security policies that provide restricted access to incumbents and candidates for your HCM data role.

1. On the Create Data Security Policies page, click **Create Data Security Policy**.
2. Complete the fields in the Create Data Security Policy dialog box using the values shown in this table.

Field	Value
Policy Name	Restricted Access to Incumbents Policy
Database Resource	Person Detail

Field	Value
Data Set	Select by instance set
Condition Name	Incumbent List Securing Condition
Actions	Create Succession Plan for Worker

3. Click **OK**.
4. Repeat steps 1 through 3 using the values shown in this table.

Field	Value
Policy Name	Restricted Access to Candidates Policy
Database Resource	Person Detail
Data Set	Select by instance set
Condition Name	Candidate List Securing Condition
Actions	Add Worker to Succession Plan

5. Click the **Summary and Impact Report** train stop.
6. Click **Save and Close** to save your changes to the HCM data role.

   To provision the HCM data role to users, create a role mapping.

   .

> **Tip:** To implement these enhancements for the Line Manager abstract role, the steps are the same except that you don't have to create a data role. As the Line Manager role is likely to have directly assigned security profiles, you edit the Line Manager role to end date the relevant data security policies.

Related Topics

- Overview of How to Secure Access to Succession Plans, Incumbents, and Candidates

Restrict Line Managers to Only View Succession Plans

As an IT Security Manager, you can ensure that line managers can only view succession plans and not edit them.

1. Remove these aggregate privileges from the Line Manager role:
    - Create Succession Plan for Worker
    - Edit Succession Plan and Manage Candidates
2. Add the **View Succession Plan** aggregate privilege to the Line Manager role.
3. Regenerate the Line Manager role on the Manage Data Role and Security Profiles page.

Related Topics

- Assign Security Profiles to Job and Abstract Roles
- Regenerate Roles

25 Securing Access to Talent Pools

Overview of Security Profiles for Talent Pools

You can use security profiles to control access to nonprivate talent pools.

You can control access to nonprivate talent pools in these ways:

- Assign any of the 3 delivered security profiles for talent pools to specific roles. For more information about this, see *Predefined HCM Security Profiles*.
- Create security profiles so that only people of a specific business unit, department, or job family can access nonprivate talent pools and then assign them to the appropriate roles. For more information about this, see *Create a Security Profile for Talent Pools* and *Assign Talent Pool Security Profiles to Specific Roles*.

Assign Talent Pool Security Profiles to Specific Roles

To override the default security profile and assign other talent security profiles to users who need to manage nonprivate talent pools, a user with IT Security Manager job role needs to associate the created talent pool security profiles with specific roles.

The delivered **View By Ownership** security profile is the default security profile for talent pools. Users assigned this profile can manage only the nonprivate talent pools that they own. Administrators can configure other security profiles for nonprivate talent pools. They can ensure that only people of a specific business unit, department, or job family can access nonprivate talent pools. Here's how you can assign these security profiles to specific roles:

1. Sign in as a user with the IT Security Manager (ORA_FND_IT_SECURITY_MANAGER_JOB) job role or privileges.
2. In the Setup and Maintenance work area, use these values:
   - Offering: Workforce Deployment
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role
3. On the Data Roles and Security Profiles page, search for and select the role for which you want to assign the talent pool security profile.
4. Edit the role.
5. On the Edit Data Role: Security Criteria page, navigate to the Talent Pool section.
6. Select any of the listed profiles or create a new profile.
7. If creating a profile, select the appropriate check boxes to secure by business unit, department, or job family.
8. Click **Next**.
9. On the Assign Security Profiles to Role page, click **Next** until you go to the Assign Security Profiles to Role: Talent Pool page.

   > **Note:** You can also directly navigate to the Talent Pool train stop.

10. If you created a new profile, add the relevant business units, departments, or job families.

11. Submit your changes.

Overview of Creating a Talent Pools Super User Job Role

This topic provides an overview of how to create a talent pools super user who can access all talent pools in your organization.

Users assigned the **View All Talent Pools** talent pools security profile can manage all private and nonprivate talent pools.

Providing Access to All Talent Pools in Your Organization

The predefined Human Resource Specialist job role enables users to access the talent pools for which they are an owner, but no predefined job role enables any user to access all talent pools. To give selected users this access, you need to create a super user job role. Then create a data role and assign the **View All Talent Pools** talent pools security profile.

Create a Talent Pools Super User Job Role

In this example, you learn how to create a job role that provides access to all talent pools in the Talent Pools work area.

The following table summarizes the key decisions for this scenario.

Decisions to Consider	In this Example
What's the name of the job role?	Talent Pools Super User
What's the code of the job role?	TALENT_POOLS_SUPER_USER_JOB
Which talent pool security profile to add?	View All Talent Pools
Do you want to enable access to Oracle Transactional Business Intelligence (OTBI) subject areas?	Yes
What's the name of the role mapping?	Access All Talent Pools
How do users acquire the role?	Users with the human resources representative responsibility can provision the role to other users.

Summary of the Tasks

Do these tasks to enable access to all talent pools in the Talent Pools work area:

1. Copy the **Use REST Service - Succession Management Lists of Values** role.
2. Create a job role.
3. Grant functional security policies to the job role.

4. Add duty roles to the custom job role.
5. Create **Talent Pool Super User** data role.
6. Enable access to OTBI subject areas.
7. Create a role mapping.

Copy the Use REST Service - Succession Management Lists of Values Role

1. Sign in with the IT Security Manager job role or privileges and select **Navigator** > **Tools** > **Security Console**.
2. On the Roles tab of the Security Console, search for and select the **Use REST Service - Succession Management Lists of Values** role.
3. Select the **Copy Role** action in the search results.
4. Select the **Copy top role** option and then click **Copy Role**.
5. On the Basic Information page, enter a unique role name and role code. By default, the copied role has the same name as its source role with the **Custom** suffix.
6. Click the **Data Security Policies** train stop.
7. Select the **Remove Data Security Policy** action for the **Data Grant on Succession Plan Detail** policy with the **Choose Succession Plan** privilege.
8. Confirm the removal.
9. Click the **Summary** train stop.
10. Click **Submit and Close**.
11. Note the process ID in the confirmation message and review the completion of the submitted process on the Role Status tab of the Administration tab of the security console. When the status is **Complete**, you can add the copied duty role to your custom job role.

Create a Job Role

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role name **Talent Pools Super User**.
3. Enter the role code **TALENT_POOLS_SUPER_USER_JOB**.
4. In the **Role Category** field, select **HCM - Job Roles**.
5. Click the **Function Security Policies** train stop.

Grant Functional Security Policies to the Job Role

1. On the Function Security Policies page, click **Add Function Security Policy** to open the Create Function Security Policy dialog box.
2. In the Create Function Security Policy dialog box, search for **HRM_CREATE_TALENT_POOL_PRIV** privilege and click **Add Privilege to Role**.
3. Close the Create Function Security Policy dialog box.
4. Click the **Role Hierarchy** train stop.

Add Duty Roles to the Custom Job Role

1. On the Role Hierarchy page, click **Add Role** to open the Add Role Membership dialog box.
2. In the Add Role Membership dialog box, search for and select the **Manage Talent Pool (ORA_HRM_MANAGE_TALENT_POOL)** role.
3. Click **Add Role Membership**.
4. Repeat steps 2 and 3 for these roles:

- **Access Talent Pool Overview (ORA_HRM_ACCESS_TALENT_POOL_OVERVIEW)**
- The custom role you created by copying the **Use REST Service - Succession Management Lists of Values** role

5. Close the Add Role Membership dialog box.
6. Click the **Summary** train stop.
7. Click **Save and Close**.

Create Talent Pool Super User Data Role

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Workforce Deployment
   - Functional Area: Users and Security
   - Task: Assign Security Profiles to Role
2. On the Data Roles and Security Profiles page, click **Create** to create a data role.
3. On the Create Data Role: Select Role page, specify these values:
   - A unique name for the data role
   - Search and select the job role you earlier created, namely **Talent Pools Super User**.
4. Click the Security Criteria train stop.
5. On the Create Data Role: Security Criteria page, from the **Talent Pool Security Profile** list, select **View All Talent Pools** security profile.
6. Review and submit the data role.

Enable Access to OTBI Subject Areas

To enable users who have the Talent Pools Super User role to access OTBI subject areas for Talent Pools, you add OTBI duty roles to the Talent Pools Super User job role and then regenerate the Talent Pools Super User data role.

1. Sign in with the IT Security Manager job role or privileges and select **Navigator** > **Tools** > **Security Console**.
2. On the Roles tab of the Security Console, search for the **Talent Pools Super User** job role.
3. In the search results, select **Edit Role** on the role's **Actions** menu.
4. Click the **Role Hierarchy** train stop and click **Add Role**.

   The Talent Pools subject area is secured with both the **FBI_SUCCESSION_MANAGEMENT_TRANSACTION_ANALYSIS_DUTY** role and the **FBI_TALENT_REVIEW_TRANSACTION_ANALYSIS_DUTY** role. Either of these two duty roles are valid.
5. If you are using the **FBI_SUCCESSION_MANAGEMENT_TRANSACTION_ANALYSIS_DUTY** role, search for it in the Add Role Membership dialog box and click **Add Role Membership.** Next, search for and select the **ORA_FBI_SUCCESSION_MANAGEMENT_TRANSACTION_ANALYSIS_DUTY_HCM** role and click **Add Role Membership**.

   If you are using the **FBI_TALENT_REVIEW_TRANSACTION_ANALYSIS_DUTY** role, search for it in the Add Role Membership dialog box and click **Add Role Membership.** Next, search for and select the **ORA_FBI_TALENT_REVIEW_TRANSACTION_ANALYSIS_DUTY_HCM** role and click **Add Role Membership**.

   To create OTBI reports, you must also have the BIAuthor role.

   Search **BI Author Role** in the Add Role Membership dialog box, select it and click **Add Role Membership**.
6. Close the Add Role Membership dialog box.

7. Click the Security Criteria train stop.
8. On the Create Data Role: Security Criteria page, from the **Person Security Profile** list, select **View All People** security profile.
9. Click **Save and Close** in the Summary train stop.
10. Regenerate the **Talent Pools Super User** data role:
    a. Search for the **Talent Pools Super User** data role.
    b. Select the role in the search results and click **Edit**.
    c. On the Edit Data Role: Select Role page, click **Next**.
    d. On the Edit Data Role: Security Criteria page, select a person security profile.
    e. On the Edit Data Role: Security Criteria page, click **Review**.
    f. On the Edit Data Role: Review page, click **Submit**.

Create a Role Mapping

You create a role mapping to enable the Talent Pools Super User Job role to be provisioned to users.

1. In the Setup and Maintenance work area, go to the following:

    - Offering: Workforce Deployment
    - Functional Area: Users and Security
    - Task: Manage Role Provisioning Rules

2. On the Role Mapping page, click the **Create** icon in the Search Results section.
3. In the **Mapping Name** field on the Create Role Mapping page, enter **Access All Talent Pools**.
4. Complete the fields in the Conditions section as shown in this table.

Field	Value
HR Assignment Status	Active
Responsibility Type	Human resources representative

5. In the Associated Roles section, click the **Add Row** icon.
6. In the **Role Name** field, search for and select **Talent Pools Super User**.
7. Select the **Requestable** option and deselect the **Autoprovision** option.
8. Click **Save and Close**.

    Users with the human resources representative responsibility can now provision the Talent Pools Super User job role to other users.

26 Securing Access to Talent Review Meetings

Overview of Creating a Talent Review Super User Job Role

This topic provides an overview of how to create a talent review super user who can access all talent review meetings in your organization.

Providing Access to All Talent Review Meetings in Your Organization

The predefined Human Resource Specialist job role enables users to access the talent review meetings for which they are a facilitator, but no predefined job role enables any user to access all talent review meetings. To give selected users this access, you can create a super user job role and provision the job role directly to those users. The job role is then granted custom data security policies that provide access to all talent review meetings.

It is not possible to configure a role that can report on all talent review meetings using Oracle Transactional Business Intelligence (OTBI).

Create a Talent Review Super User Job Role

In this example, you learn how to create a job role that provides access to all talent review meetings in the Talent Review Meetings work area.

The following table summarizes key decisions for this scenario.

Decisions to Consider	In this Example
What's the name of the job role?	Talent Review Super User
What's the code of the job role?	TALENT_REVIEW_SUPER_USER_JOB
What are the names of the data security policies?	Talent Review Custom Policy
What is the name of the role mapping?	Access All Talent Review Meetings
How do users acquire the role?	Users with the human resources representative responsibility can provision the role to other users.

Summary of the Tasks

Enable access to all talent review meetings in the Talent Review Meetings work area by:

1. Creating a job role
2. Granting functional security policies to the job role
3. Granting data security policies to the job role
4. Creating a role mapping

Create a Job Role

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role name **Talent Review Super User**.
3. Enter the role code **TALENT_REVIEW_SUPER_USER_JOB**.
4. In the **Role Category** field, select **HCM - Job Roles**.
5. Click the **Function Security Policies** train stop.

Granting Functional Security Policies to the Job Role

1. On the Function Security Policies page, click **Add Function Security Policy** to open the Create Function Security Policy dialog box.
2. In the Create Function Security Policy dialog box, search for **HRR_CONDUCT_TALENT_REVIEW_PRIV** privilege and click **Add Privilege to Role**.
3. Search for another privilege, **HRR_SCHEDULE_TALENT_REVIEW_MEETING_PRIV** and click **Add Privilege to Role**.
4. Click the **Data Security Policies** train stop.

Granting Data Security Policies to the Job Role

1. On the Data Security Policies page, click **Create Data Security Policy** to open the Create Data Security Policy dialog box.
2. In the Create Data Security Policy dialog box, enter the policy name **Talent Review Custom Policy**.
3. Search for and select the database resource **Talent Review Meeting (HRR_MEETINGS)**.
4. Select **All values** in the **Data Set** field.
5. Select **Schedule Talent Review Meeting** in the **Actions** field.
6. Click **OK** to close the Create Data Security Policy dialog box.

Create a Role Mapping

You create a role mapping to enable the Talent Review Super User Job Role to be provisioned to users.

1. In the Setup and Maintenance work area, go to the following:

   - Offering: Workforce Deployment
   - Functional Area: Users and Security
   - Task: Manage Role Provisioning Rules

2. On the Role Mapping page, click the **Create** icon in the Search Results section.
3. In the **Mapping Name** field on the Create Role Mapping page, enter **Access All Talent Review Meetings.**.
4. Complete the fields in the Conditions section as shown in this table.

Field	Value
HR Assignment Status	Active
Responsibility Type	Human resources representative

5. In the Associated Roles section, click the **Add Row** icon.
6. In the **Role Name** field, search for and select **Talent Review Super User**.
7. Select the **Requestable** option and deselect the **Autoprovision** option.
8. Click **Save and Close**.

   Users with the human resources representative responsibility can now provision the Talent Review Super User Job Role to other users.

27 Security and the Responsive User Experience

Privileges and Roles Securing Lists of Values in Responsive User Experience Pages

Function security privileges, aggregate privileges, and duty roles secure access to lists of values in the responsive user experience pages. Predefined job and abstract roles inherit these privileges and roles. If you're using the predefined roles, then no action is necessary.

If you're using both the responsive user experience pages and custom versions of relevant roles, then you must add these privileges and roles to your custom roles. For a list of the privileges and duty roles, lists of values that they secure, and the predefined roles that inherit them, see the *Authorize* topic under the **Get Started** section in the *REST API for Oracle Fusion Cloud HCM* guide.

Related Topics

- Edit Job Role and Abstract Role
- HCM Responsive Edit Page Demos (Doc ID 2399671.1)
- Managing Role Definitions Using CSV File Packages

Overview of Quick Actions

This topic provides a brief overview of Quick Actions and how they're secured using privileges.

Tabs in the `Newsfeed` Home Page that comes with the HCM Responsive User Experience are visible if the user has access to one or more applications that sit on the respective tabs.

Quick Actions exist for the Me, My Team, and My Client Groups tabs. Sometimes, a Quick Action sits on more than one tab. If any of the tabs is visible, then the Quick Actions to which the user has been granted access are displayed on the selected tab.

Quick Actions are secured using privileges. Sometimes the privileges that secure the Quick Actions are tab-specific, meaning that each instance of a Quick Action within a tab is secured with a unique privilege. And sometimes a Quick Action is secured with a single privilege, even if the Quick Action is available on more than one tab. For example, the Employment Info Quick Action is secured using the aggregate privilege View Employment Information Summary (`ORA_PER_VIEW_EMPLOYMENT_INFORMATION_SUMMARY`). This aggregate privilege is granted to a number of predefined roles, including Employee (ORA_PER_EMPLOYEE_ABSTRACT), Line Manager (ORA_PER_LINE_MANAGER_ABSTRACT), Human Resource Specialist (ORA_PER_HUMAN_RESOURCE_SPECIALIST_JOB), and Human Resource Analyst. It sits on the Me, My Team, and My Client Groups tabs.

A user with only the Employee role sees the Me tab, but not My Team or My Client Groups. In this scenario, the user sees the Employment Info Quick Action on the Me tab. If the user is given a Learning Specialist data role, then the My Client Groups tab is visible, because the Learning Specialist role grants access to the Learning application, which sits on the

My Client Groups tab. The Employment Info Quick Action is visible on the My Client Groups tab. When the user clicks on My Client Groups > Employment Info, the worker list of values shows assignments for just the logged in user. This is because, of the two roles the user has been assigned, only Employee has the View Employment Information Summary aggregate privilege.

Considering another example, the Personal Details Quick Action is secured using two aggregate privileges: Access Personal Details by Worker (ORA_PER_ACCESS_PERSONAL_DETAILS) and Access Personal Details by HR (ORA_PER_ACCESS_PERSONAL_DETAILS_BY_HR). The first aggregate privilege secures the Quick Action on the Me tab, and the second aggregate privilege secures the Quick Action on the My Client Groups tab. Access Personal Details by Worker is granted to the Employee and Contingent Worker roles. Access Personal Details by HR is granted to the Human Resource Specialist and Human Resource Analyst roles.

A user who has the Employee role plus a Learning Specialist data role sees the Me tab and the My Client Groups tab, but the Personal Details Quick Action only appears on the Me tab.

You can find the aggregate privileges granted to predefined job and abstract roles documented in the guide *Security Reference for Oracle HCM Cloud*.

Related Topics

- Configure Quick Actions
- Sign In and Get Started

28 Security and Reporting

Oracle Fusion Transactional Business Intelligence Security

Oracle Fusion Transactional Business Intelligence is a real-time, self-service reporting solution. Application users with appropriate roles can use Transactional Business Intelligence to create analyses that support decision making. Business users can also perform current-state analysis of their business applications using various tools.

These include Oracle Business Intelligence Enterprise Edition as the standard query and reporting tool, Oracle Business Intelligence Answers, and Oracle Business Intelligence Dashboard 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:

- The Workforce Management folder in the Business Intelligence Catalog

- 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

Reporting-Data Security

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 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 role must access the Workforce Transaction Analysis subject areas, then it must inherit the duty roles shown in this table.

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

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 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.

Business Intelligence Role	Description

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 have 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.

View Reporting Roles and Permissions

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

View Inherited Reporting Roles on the Security Console

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

1. 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.

2. 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.
3. 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.
4. Notice that the Absence Management Transaction Analysis Duty role inherits BI Consumer Role. Most of the **OBI** duty roles inherit BI Consumer Role.
5. 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.

View 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 inherit BI Administrator Role.

1. 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

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 from the Report menu.

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 email, 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 shown 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 shown 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 shown in this table.

Table	Secured List View	Data Security Privilege
HR_ALL_ORGANIZATION_UNITS_F	PER_LEGAL_EMPL_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 privilege shown in this 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 shown in this 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

Personally identifiable information (PII) data is secured at the database level using virtual private database (VPD) policies. Only authorized users can report on PII data. This restriction also applies to Oracle Business Intelligence Publisher reports.

PII data 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 those 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
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 email 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

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 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 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.

29 Roles for Workflow Access

Roles for HCM Workflow Access

Predefined roles provide access to workflow functionality. Users with these roles can, for example, set up approval rules and manage submitted approval tasks.

This table identifies the predefined Oracle Business Process Management (BPM) role for HCM workflow access and the predefined job role that inherits it. You can assign the predefined BPM role to a custom job role, if required.

BPM Role Name	BPM Role Code	Inherited by Job Role
BPM Workflow Human Capital Management Administrator	BPMWorkflowHCMAdmin	Human Capital Management Application Administrator (ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_APPLICATION_ADMINISTRATOR_JOB)

The role BPM Workflow All Domains Administrator Role (BPMWorkflowAllDomainsAdmin) provides workflow access for all Oracle Fusion product families. This role isn't assigned to any predefined job role, but you can add it to custom job roles.

For more information about how to secure access to Transaction Console, see the topic *Transaction Security Profiles*.

Related Topics

- Transaction Security Profiles

30 Auditing Oracle HCM Cloud Business Objects

How You Audit Oracle HCM Cloud Business Objects

You can record and later retrieve audit information about the creation, update, and deletion of Oracle HCM Cloud business objects. Audit information can be recorded, regardless of whether business objects are created individually or by bulk upload.

This audit information is stored without user intervention. This topic summarizes how to manage audit policies and access the audit reports.

Audit Policies

You create audit policies to identify:

- Business objects to audit
- The attributes of the selected business objects to audit

Therefore, you can audit changes to a subset of a selected business object's attributes, if appropriate.

Enabling and Disabling Audit

By default, auditing is disabled for all applications. To enable auditing for Oracle HCM Cloud, you:

1. Configure business objects for audit on the Configure Business Object Attributes page.
2. Enable auditing for Oracle Fusion Applications on the Manage Audit Policies page.

Auditing begins for the specified objects immediately.

To stop auditing an entire object, you can deselect the object on the Configure Business Object Attributes page. You can also select different attributes for audit at any time. If necessary, you can disable all auditing for Oracle Fusion Applications on the Manage Audit Policies page.

To manage audit, you must have the Manage Audit Policies (FND_MANAGE_AUDIT_POLICIES_PRIV) function security privilege. The predefined Application Implementation Consultant job role has this privilege.

Audit Reports

To access the data recorded by the audit process, you view audit reports in the Audit Reports work area. To open the Audit Reports work area, select **Navigator** > **Tools** > **Audit Reports**.

To view audit reports, you must have the View Audit History (FND_VIEW_AUDIT_HISTORY_PRIV) function security privilege. The predefined Internal Auditor job role has this privilege.

Related Topics

- Enable Audit for Oracle HCM Cloud Business Objects
- Auditable Oracle HCM Cloud Business Objects
- Audit Reports

Enable Audit for Oracle HCM Cloud Business Objects

This procedure describes how to enable audit for selected HCM business objects.

Select Products to Audit

Follow these steps:

1. In the Setup and Maintenance work area, search for and click the **Manage Audit Policies** task.
2. On the Manage Audit Policies page, click **Configure Business Object Attributes** in the Oracle Fusion Applications section.
3. On the Configure Business Object Attributes page, select a product. For example, set **Product** to **Profile Management**.

   When you select a product, the objects that you can audit are listed in groups in the Objects section of the page. For example, for Profile Management you see:

   - Audit Top Node
     - Talent Content Library
     - Talent Pools
     - Talent Profiles
     - Talent Profiles Setup
     - Common Notes

   Under each of these object groups, you see hierarchies of objects and their auditable components. For example, in the Talent Content Library group you see this hierarchy:

   - Rating Models
     - Rating Levels
   - Content Items

Select Objects and Attributes to Audit

Follow these steps:

1. In the **Audit** column of the table of business objects, select an item to audit. These rules apply:
   - When you select a single component, such as **Rating Levels**, its object group and **Audit Top Node** are selected automatically.
   - When you select an object group, such as **Talent Content Library**, every entry in the group and **Audit Top Node** are selected automatically.

    - If you select **Audit Top Node**, then every object group and its contents are selected automatically.

2. You can configure the attributes to audit only when you select a single component, such as **Rating Levels**. When you select a single component, the Audited Attributes section of the page is updated automatically to list the attributes that are audited by default. To update the list of attributes, click the **Create** icon.

   The Select and Add Audit Attributes dialog box opens.
3. In the Select and Add Audit Attributes dialog box, you can deselect the selected attributes, if appropriate, and select additional attributes. To audit flexfield attributes, if any, select the **Flexfields (Additional Attributes)** option in the dialog box. This option appears only if the selected component has flexfields.
4. Click **OK** to close the dialog box.
5. Click **Save and Close** on the Configure Business Object Attributes page.

Enable Audit

On the Manage Audit Policies page:

1. Set **Audit Level** to **Auditing**.
2. Click **Save and Close** to close the Manage Audit Policies page.

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

Related Topics

- How You Audit Oracle HCM Cloud Business Objects
- Auditable Oracle HCM Cloud Business Objects

Auditable Oracle HCM Cloud Business Objects

This topic lists the Oracle HCM Cloud business objects that you can audit.

This table lists the business objects that you can audit for each product.

Product	Object
Absence Management	Absence Records
Compensation	Salary
Employee Wellness	• Activities • Wellness User
Global Human Resources	• Business Unit • Checklist • Common Work Structure • Data Role

Product	Object
	• Document Records • Eligible Jobs • Grade • Health and Safety • Job • Location • Organization • Person • Position • Role Delegation • Security Profiles • Seniority Dates • Worker Employment
Global Payroll	• Pay Core Audit • Pay Security Profile
Oracle Fusion Middleware Extensions for Applications	• Attachments • Data Security • Descriptive Flexfields • Document Categories • Document Entities • Key Fiexfields • Lookups • Profiles
Performance Management	• Check In Meeting • Performance Evaluations
Profile Management	• Common Notes • Talent Content Library • Talent Pools • Talent Profiles • Talent Profiles Setup
Recruiting	• Description • Requisition
Succession Management	Succession Plans
Workforce Health and Safety Incidents	• Health and Safety Action • Health and Safety Incident Core

Product	Object
	• Health and Safety Incident Event • Health and Safety Incident Kiosk

To configure the object components and attributes to audit for each business object, perform the **Manage Audit Policies** task.

Related Topics

- How You Audit Oracle HCM Cloud Business Objects
- Enable Audit for Oracle HCM Cloud Business Objects

Enable Audit for Oracle Platform Security Services

You can record and later retrieve audit information about changes that are made to role definitions and changes to user role assignments. This audit information is stored without user intervention. This topic summarizes how to enable Oracle Platform Security Services audit, and how to access the audit reports.

Enabling and Disabling Audit

By default, auditing is disabled for all applications. To enable auditing for Oracle Platform Security Services, follow these steps:

1. In the Setup and Maintenance work area, search for and click the **Manage Audit Policies** task.
2. On the **Manage Audit Policies** page, set **Audit Level** to **Low - Critical Events Only** for Oracle Platform Security Services.
3. Click **Save and Close** to close the **Manage Audit Policies** page.

To disable auditing for Oracle Platform Security Services, set **Audit Level** to **None**.

To manage audit, you must have the Manage Audit Policies (FND_MANAGE_AUDIT_POLICIES_PRIV) function security privilege. The predefined Application Implementation Consultant job role has this privilege.

Audit Reports

Use the Security - Audit Real Time subject area to access the Oracle Platform Security Services audit data. To access this Oracle Transactional Business Intelligence (OTBI) subject area you must have the FBI_SECURITY_TRANSACTION_ANALYSIS_DUTY duty role. The predefined IT Security Manager job role has this duty role. You can also use this subject area to report on data security audit data for the Oracle Fusion Middleware Extensions for Applications product.

Options for Enabling Access to HCM Audit Data

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 Job Roles

Your enterprise might 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 version of the job role to which you add the relevant privileges. You include this custom job role in an HCM data role with one or more security profiles that identify the data.

Sensitive Data Access Audit

You can audit the viewing of sensitive data in the HCM Responsive pages. You can use this information for compliance and monitoring of access to sensitive data from your browser.

Read access to the following sensitive attributes can be audited:

- National Identifier Number
- Passport Number
- Driver License Number
- Personal Home Address
- Personal Email Address
- Personal Telephone Number
- Other Communication Account
- Citizenship Number
- Visa Number, Work Permit, and Residency Number

The Sensitive Data Access Audit page is secured using a function security privilege with a privilege code of PER_VIEW_SENSITIVE_DATA_ACCESS_AUDIT_PRIV. It's granted to the predefined IT Auditor role. If you want to allow any custom job or abstract roles to access this page, you should grant this function security privilege to the custom roles.

Function Security Privilege	Predefined Role
PER_VIEW_SENSITIVE_DATA_ACCESS_AUDIT_PRIV	IT Auditor

Enable Sensitive Data Access Audit

To enable auditing of sensitive data access, you need to set the Mobile-Responsive Sensitive Data View Audit Enabled (ORA_HCM_SENSITIVE_DATA_VIEW_AUDIT_ENABLED) profile option to Y.

1. Go to the **Setup and Maintenance** work area.
2. Search for and click the **Manage Administrator Profile Values** task.
3. Search for the **ORA_HCM_SENSITIVE_DATA_VIEW_AUDIT_ENABLED** profile option code and select it from the search results.
4. Below, set the **Profile Level** to **site** and the **Profile Value** to **Y**.
5. Click **Save and Close**.

The sensitive data access audit information for a user session is available after the user has signed out of Oracle HCM Cloud, or their session has timed out, or they have performed more than 20 clicks.

Auditing Talent Pool Security Profiles

Configure Auditing for Talent Pool Security Profiles

Auditing security profiles created for talent pools helps you to track their changes and manage them better.

To configure auditing of security profiles created for talent pools, ensure that you're assigned a role with the **Manage Audit Policies** (**FND_MANAGE_AUDIT_POLICIES_PRIV**) privilege.

1. Go to the Setup and Maintenance work area.
2. Search for and select the **Manage Audit Policies** task.
3. On the Manage Audit Policies page, ensure that the audit level is set to **Auditing**.
4. Click **Configure Business Object Attributes**.
5. On the Configure Business Object Attributes page, select the **Succession Management** product.
6. Ensure that the **Audit Top Node** is selected.
7. Select **Talent Pool Security Profile Audit Objects** and then **Talent Pool Security Profile**.

   > **Note:** You need to select the parent node first. Then, you can select any of its child nodes.

8. The **Name** attribute is selected by default for the Talent Pool Security Profile Audit Objects. To add another attribute, do these steps:
   a. Click the **Add** icon in the Actions area of the Audited Attributes region or click **Actions** > **Create**.
   b. Click the search icon and then select the attributes that you want to include.
   c. Click **OK**.
9. The **Pool Security Profile ID** attribute is selected by default for the Talent Pool Security Profile object. You can add other attributes using the steps listed in Step 8.
10. Click **Save and Close** to save the audit profile.

Related Topics

- How You Audit Oracle HCM Cloud Business Objects
- Enable Audit for Oracle HCM Cloud Business Objects

View Audit Reports for Talent Pool Security Profiles

You can view audit reports only for talent pool security profiles that are enabled for auditing.

To view or generate an audit report, you need to have a role with the **View Audit History** (**FND_VIEW_AUDIT_HISTORY_PRIV**) privilege assigned to it.

1. Click **Navigator** > **Tools** > **Audit Reports**.
2. On the Audit Reports page, enter the search criteria. Select the **Succession Management** product.
3. Select the talent pool security profile business object types that you want to audit. Select the **Include child objects** check box if you want the child objects also to be audited.
4. Click **Search**.

Results:

You can export the audit results to an Excel or CSV file.

Related Topics

- Audit Reports
- View Audit Reports

31 Certificate Management

Overview of Certificates

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.

Click the Actions menu to take an appropriate action for a certificate. 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.

Types of Certificates

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 type of generated key: DSA or RSA.
- Key length: 512, 1024, or 2048.
- Encryption algorithm option for key generation: AES128, AES256

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 doesn't 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.

Sign a X.509 Certificate

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 doesn't 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.

Import and Export X.509 Certificates

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're 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're 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.

Related Topics

- Sign a X.509 Certificate

Import and Export PGP Certificates

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 wouldn't 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 doesn't 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're importing).
3. Browse for the public-key file, then select Import and Close.

The following PGP certificate formats aren't supported:

- GnuPG v2.0.22 (GNU/Linux)
- Keybase OpenPGP v1.0.0
- OpenPGP.js v4.10.10

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 don't 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.

Delete Certificates

You can delete both PGP and X.509 certificates. On 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.

In either menu, select Delete. 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.

32 Advanced Data Security

Advanced Data Security

Advanced Data Security offers two types of added data protection. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest.

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and application 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 can't select from the application tables. If a DBA requires access to the application tables, request temporary access to the Oracle Fusion schema at which point keystroke auditing is enabled.

Transparent Data Encryption

Transparent Data Encryption (TDE) protects Oracle 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.