Oracle Fusion Cloud HCM

How do I configure data roles and security profiles?

Oracle Fusion Cloud HCM
How do I configure data roles and security profiles?

G35727-04

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

Some application pages have help icons to give you access to contextual help. 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. If the page has contextual help, help icons will appear.

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.

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 Introduction

About this Playbook

Use this playbook as your go-to guide for understanding, creating, and managing data roles and security profiles in a way that makes sense for your organization.

Whether you're new to data security or looking to refine your approach, this playbook is designed to break down these critical concepts in a simple, hands-on way. We'll walk you through everything you need to know — from understanding the basics of data roles and security profiles, to best practices, and even role delegation. By the end of this guide, you'll have the tools to create a secure, efficient system that aligns with your organization's needs.

You might be wondering: *Why are these topics so important?* Well, data roles and security profiles are the backbone of controlling access to your organization's sensitive information. Without them, it's easy for things to get chaotic. Misconfigured roles can lead to unauthorized access, or worse, data breaches. But don't worry — this guide will walk you through the entire process, step-by-step, so you can avoid common pitfalls and set up a solid structure.

In the following chapters, we'll cover:

- **Data Roles**: What they are, why they matter, and how to define them.
- **Security Profiles**: How they tie into data roles and how to use them effectively.
- **Predefined Security Profiles**: Understanding ready-made profiles and how to tweak them for your needs.
- **Previewing HCM Data Security**: How to preview data security to help diagnose problems with accessing secured data.
- **Configuring Data Roles and Security Profiles for Audit**: How to configure the attributes of HCM data roles and security profiles for audit.
- **Creating Your Own Data Roles**: How to configure roles from scratch for the best results.
- **Regenerating Security Profiles**: How to regenerate a security profile when it's required for a new feature.
- **Best Practices for Security Profiles and Data Roles:** Proven tips and strategies for smooth and secure configurations.

Ready to dive in? Let's get started!

2 Data Roles and Security Profiles

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 **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.

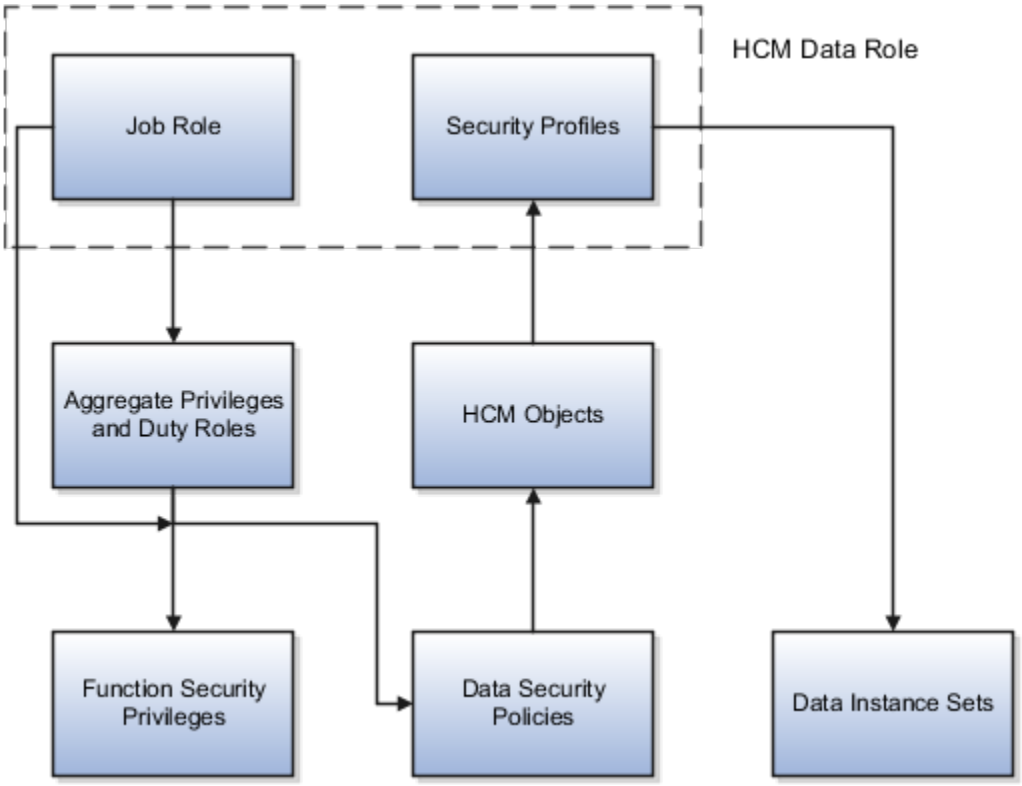
> **Note:** You must ensure that the job role doesn't have directly assigned security profiles. Search for the job role on the **Data Roles and Security Profiles** page. In the search results, confirm that no check mark appears in the **Security Profiles Assigned** column. If security profiles are assigned 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.

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 might 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 the **Position Security Profiles** task in the 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.

Predefined 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
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

Security Profile Name	Security Profile Type	Data Instance Set
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 a 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 might 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 **Data Roles and Security Profiles**.
3. In the Search Results section of the **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

Field	Value
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 **Data Roles and Security Profiles** page, you can search for the new HCM data role to confirm that it was created successfully. When the role's status is **Complete**, you can assign the role to your HR specialists.

Edit a 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.

Best Practices for 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 might 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.

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 **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. Navigate to **Tools** > **Scheduled Processes**.
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 mark a role for delegation by using the **Security Console**. In the **Users** tab, search and view the selected user account details and edit. In the roles table there's an **Assignable** option for each role listed. After the **Assignable** option is selected for the role, the role is marked for delegation. 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've currently, if the role is enabled for delegation.

> **Note:** The role might 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, if 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've 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 might 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 during 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 isn't 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 might 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.

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

  or

- The **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 hasn't 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's 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's 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 can 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. Or, 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.

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's 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
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'll 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.

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. Select **Navigator** > **My Client Groups** > **Workforce Structures** > **Data Roles and Security Profiles**.
2. On the **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 **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 might 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 might have assigned security profiles directly to a job role and included the job role in a data role later. In this case, users might have access to more data than you intended. Follow these steps to remove security profiles from a role:

1. On the **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.

Preview HCM Data Security

On occasion, users might 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 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 might 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. Or, 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 enough for you to diagnose and resolve most data-access issues.

Configure 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.

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
COUNTRY	Country

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