Oracle Fusion Cloud HCM

How do I secure person records in HCM?

Oracle Fusion Cloud HCM
How do I secure person records in HCM?

G38899-01

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 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 Introduction

Understanding Person Security in HCM

Securing person records in HCM systems is a critical component of data privacy, regulatory compliance, and internal access control.

This playbook is designed to provide a clear, practical framework for implementing and managing person security profiles using tools like custom criteria, exclusion rules, and area of responsibility (AOR). Whether you're configuring person types, designing exclusion logic, or securing records by geographical or organizational boundaries, this guide offers actionable insights and reference materials to help you secure sensitive employee data effectively.

2 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.

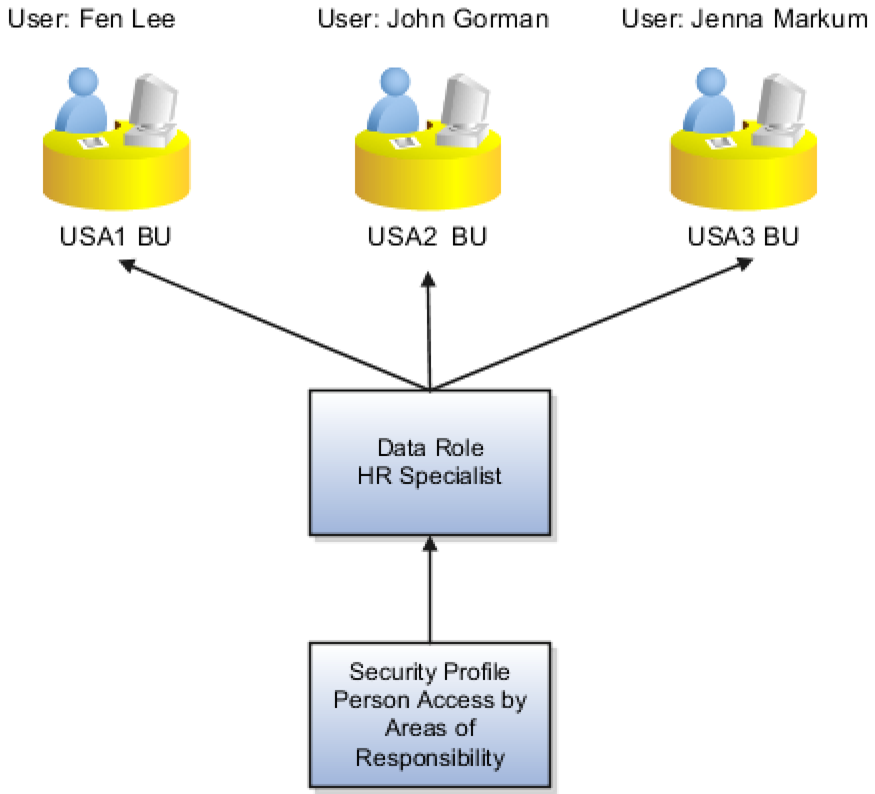
For example, consider the human resource (HR) specialists shown in this table. They perform the same job role but for workers in different business units.

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 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.

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'd need 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.

Create the Person Security Profile

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

> **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've 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

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

> **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.

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.

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've 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

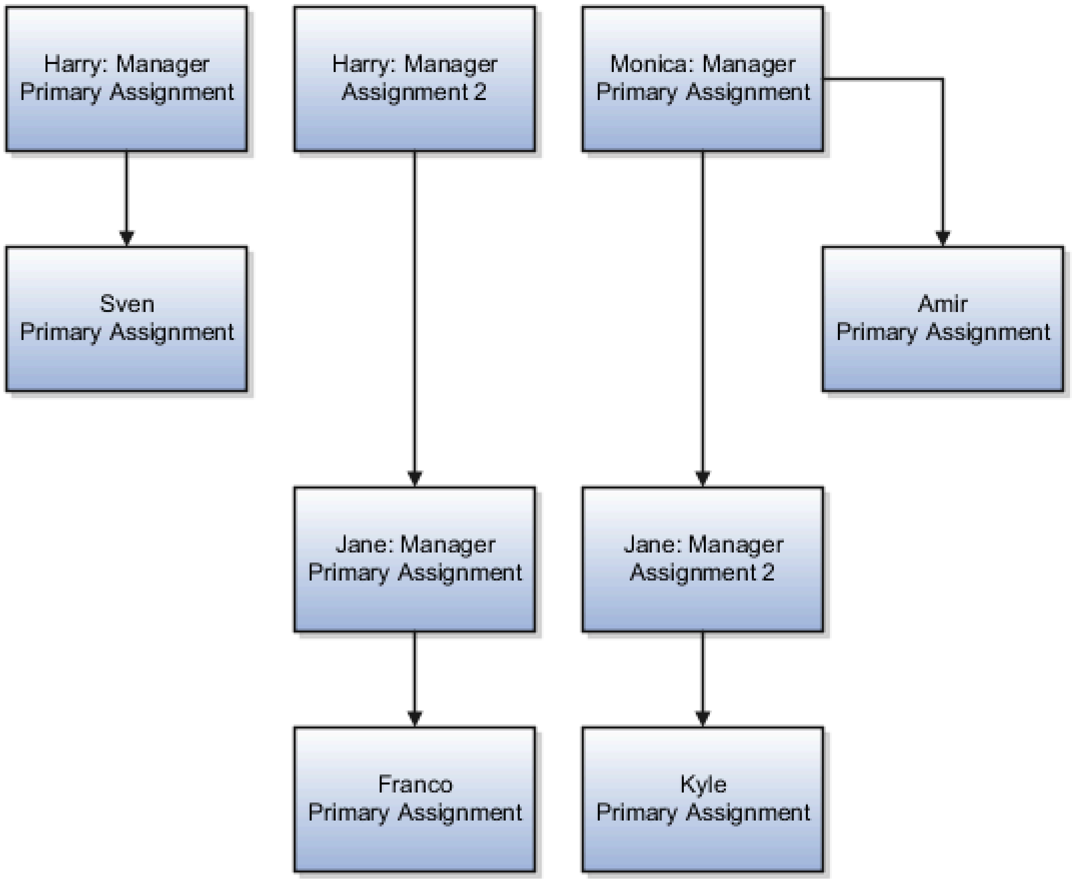
The person records that a manager can access depend on how you specify the manager hierarchy in the person security profile. This topic describes the effect of the Person or Assignment Level option, which you set to either Person or Assignment.

> **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 everyone in their 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.

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.

Manager Type	Description
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 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 their 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.

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 their 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 Attribute 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's 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's 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.

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. Or, 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.

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_ • PER_ADDRESSES_F_SEC • PER_CONT_WORKERS_CURRENT_X • PER_CONT_WORKERS_X • PER_DISPLAY_PHONES_V

Product	Table or View
	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
Grants Management	GMS_ALL_CONTACTS_V GMS_INTERNAL_CONTACTS_V
Payments	IBY_EXT_FD_EMP_HOME_ADDR

Product	Table or View
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*.

Exclude Some Records from a Person Security Profile

To exclude some records, 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.