Oracle Fusion Cloud Talent Management

How do I set up Succession Management for Redwood ?

Oracle Fusion Cloud Talent Management
How do I set up Succession Management for Redwood ?

G27667-01

Author: Malini Sampathkumar

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 Overview

Overview of Setting Up Redwood Succession Management

Use this playbook to set up Redwood Succession Management for your organization. To implement Redwood Succession Management, you need to have the privileges of an application implementation consultant.

Do these tasks to set up Redwood Succession Management:

- Enable Redwood Succession Management. For more information on this, see *Set profile options for Redwood pages*.
- *Configure readiness levels for succession plan candidates*.
- *Configure relevant descriptive flexfields*.
- *Configure alerts for Succession Management*.
- *Schedule the **Succession Plan Incumbents** process*.
- *Enable succession organization charts*.
- *Secure access to succession plans, incumbents, and candidates*.
- *Enable AI-recommended succession candidates*.
- *Extend Succession Management pages using Visual Builder Studio.*

2 Configure Lookups and Descriptive Flexfields

Configure Readiness Levels for Succession Plan Candidates

The readiness level for a succession plan candidate indicates the time that's needed for the candidate to move to the job or position defined in the succession plan.

1. Use the **Succession Management Lookups** task in the Setup and Maintenance work area.
2. Click the **HRM_READINESS_CATEGORY** lookup.
3. Add lookup codes for the readiness levels that your organization needs.
4. Save your changes.

Descriptive Flexfields for Succession Management

To add company-defined attributes, for example more information about succession plans or candidates, use descriptive flexfields for an Oracle Fusion Cloud Succession Management entity. You can use descriptive flexfields to define validation and display properties.

Defining Descriptive Flexfield Segments

Use the Manage Descriptive Flexfields task to define a segment for a descriptive flexfield for the succession management business process. You can add more information related to these succession management entities, such as the succession plan details and candidates.

Two descriptive flexfields are available in the succession management business process.

Descriptive Flexfield	Description
HRM_PLANS	Fields for succession plan details that appear in the Plan Info section of a succession plan.
HRM_PLAN_CANDIDATES	Fields for candidate details that appear in the Candidates section of a succession plan.

Related Topics

- Overview of Descriptive Flexfields
- Overview of Flexfields

3 Succession Management Alerts

How You Configure Alerts for Succession Plans

As an administrator, you might want to alert owners of a succession plan about assignment changes of candidates or incumbents.

Use the **Succession Plan Assignment Change Alert** templates in Alerts Composer to configure alerts for succession plans.

These alerts can help plan owners decide if they need to update the succession plans. For example, if a candidate moves to a role that's different from the plan role, the plan owner can remove that candidate and add other candidates to the succession plan after receiving the alert notification.

By default, all the succession plan related alerts are disabled. You need to enable the alert for users to receive the notification.

> **Note:** Although you can add new templates in Alert Composer for succession plans, these new templates won't trigger any notifications.

Alerts for Assignment Changes

You can configure alerts for these assignment changes:

- A candidate's job changes to the job specified in the succession plan.
- A candidate moves to a job that's different from the job specified in the succession plan.
- The plan incumbent moves to a different role.
- A candidate moves to a position that's different from the position specified in the succession plan.
- A candidate's position changes to the position specified in the succession plan.
- A candidate moves to a role different from the plan incumbent's role.
- A candidate moves to a job that's the same as the plan incumbent's job.

Allowed Actions for Succession Plan Alerts Templates

The succession plans alert template is extensible. This table lists the actions that you can do with the template.

Action	Can Do?
Disable the delivered alerts.	Yes
Change the text of the subject line and the message in the alert.	Yes
Change the expressions used in the subject line or message.	No

Action	Can Do?
Delete the delivered template.	No
Change the template name or the communication method.	No

How You Send Succession Alerts on Role Change Effective Date

Your organization might want to notify plan owners about incumbent and candidate role changes or employment terminations after they become effective. This enables succession plan owners to keep the succession plans up to date.

If the assignment changes or employment terminations are effective on or before the current date, then alerts are sent to the plan owners automatically.

But for future-dated assignment changes or employment terminations, you need to schedule the **Notify After Processing Effective Assignment Changes and Terminations** process regularly. This ensures that alerts are sent for assignment changes or employment terminations that become effective on or before the date the process is run. Note that to run this process, you need to have a role that inherits the **Run Global HR Processes** function security privilege.

After You Run the Process

Here's what happens after the **Notify After Processing Effective Assignment Changes and Terminations** process runs successfully:

- Owners receive notifications on the day these role changes or employment terminations become effective if the process is run daily:
  - Plan incumbent moves to a different role
  - A candidate moves to the plan role
  - A candidate moves to a role that's different from the plan role or their employment is terminated

  > **Note:** Owners receive notifications only if all these conditions are true:
  > - Alerts are enabled using the **Succession Plan Assignment Change Alert** or the **Removal of Candidate from Plans Alerts** alert event in Alerts Composer.
  > - Alerts are enabled in the Alerts section of the succession plan.
  > - Notifications are enabled for the owners in the Owners section of the succession plan.

- When owners view a succession plan, they see banners for the effective role changes of incumbents and candidates.

- Processed notification records for the incumbent and candidate role changes that are older than 90 days are deleted.

Related Topics

- Submit Scheduled Processes and Process Sets

4 Schedule the Succession Plan Incumbents Process

Ensure that the incumbents listed in your succession plans are the latest by regularly scheduling the **Succession Plan Incumbents** process.

1. Click **Navigator** > **Tools** > **Scheduled Processes**.
2. On the Scheduled Processes Overview page, click **Schedule New Process**.
3. Leave the type as **Job**.
4. Search for and select the **Succession Plan Incumbents** process.
5. Optionally, in the Process Details dialog box, change the process schedule to one that's appropriate for your organization and define notifications.

   By default, the **Succession Plan Incumbents** process is scheduled as soon as possible.
6. In the Process Details dialog box, click **Submit**.

5 Enable Succession Organization Charts

Enable Succession Organization Charts

A succession organization chart provides information about succession plans of a manager and persons reporting to the manager.

To enable succession organization charts, do these tasks:

1. Enable the **Succession Organization Chart Enabled** profile option.
2. Grant the relevant privilege.
3. *Schedule the Succession Plan Incumbents process* regularly to ensure that the details shown on the succession organization chart are the latest.

Enable Profile Option

Here's how you enable the **Succession Organization Chart Enabled** profile option:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. Search for and select the **Succession Organization Chart Enabled** (**ORA_HRM_ENABLE_SUCCESSION_ORG_CHART**) profile option.
3. Specify the level at which the profile value is to be set as **Site**.
4. In the Profile Values section, enter **Y** in the **Profile Value** column.
5. Click **Save and Close**.

Grant Relevant Privilege

The users who need to use succession organization charts need to have a role that inherits the **Use REST Service – Succession Org Charts REST** aggregate privilege. After you add this privilege, you must regenerate the grants for the data role.

6 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.

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.

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

How You Enable Managers to Manage Their Succession Plans

Your organization might want to allow some managers to create and manage their own succession plans.

The predefined Line Manager role with the **View Manager Hierarchy** person security profile doesn't allow managers to edit their own records. So, you need to create a custom role with a different security profile that allows managers to manage their own succession plans. You then need to assign this custom role to managers in addition to their predefined Line Manager role.

1. Create a custom abstract role. For more instructions, see the *Create Job Role and Abstract Role from Scratch* topic.
2. Add these aggregate privileges to the custom abstract role:
    - Create Succession Plan for Worker
    - Edit Succession Plan and Manage Candidates
3. Assign the predefined **View Own Record** person security profile to this custom abstract role. For more instructions, see the *Assign Security Profiles to Job and Abstract Roles* topic.
4. Provision the role to managers who need to manage their own succession plans. For more information, see the *Role Provisioning and Deprovisioning* topic.

Related Topics

- Edit Job Role and Abstract Role

7 Enable AI-Recommended Succession Candidates

Activate AI App

To view AI-based candidate recommendations for succession plans, you need to activate the Oracle AI Talent Best Match app.

1. On the home page, click the Tools tab and then click the **AI Apps Administration** quick action.
   On the Application Administration page, you can see a list of apps and their current activation status.
2. From the **Product Family** list, select **Human Capital Management**.
3. Locate the AI Talent Best Match app and click the row.
4. Click **Activate App**.

Synchronize Succession Plans Data for AI Recommendations

You need to schedule the Synchronize Talent Data for AI Recommendations process regularly to view AI-based candidate suggestions for succession plans.

1. Sign in as an admin user with the PER_RUN_HR_PROCESSES_PRIV privilege.
2. From either the Tools tab or from the navigator, select **Scheduled Processes** .
3. On the Scheduled Processes Overview page, click **Schedule New Process**.
4. Select the type as **Job**.
5. Search for and select the **Synchronize Talent Data for AI Recommendations** process.
6. Provide the parameters according to this table.

Parameter	Value
AI Feature	Best Profile Matches
Talent Object	Select **All** to ingest all object types. You may optionally choose to ingest one talent object at a time.
From Date	Indicates the date from which we want the Talent Object data to be pushed to AI cloud. When left blank, an incremental ingestion will pick the Talent Object data from the last successful run.
Number of Threads	Select the number of parallel java processes to run during ingestion. Use the default value unless you've a specific reason to select a different value. Default: 8, Minimum: 1, Maximum: 20

Parameter	Value
Submission Notes	Provide optional comments regarding the current scheduled process.

7. Click **Submit**.
8. Use the refresh icon to track recently submitted jobs.

Results:

After the scheduled process completes, anonymized data from HCM Cloud would have been exported to the AI cloud service. Processing of this data will begin automatically and is expected to take about 8-12 hours to complete, depending on the volume of data. You can start seeing candidate recommendations after this process completes.

Set Up Suggested Successor

When you enable Artificial Intelligence (AI) based candidate suggestions for succession plans, succession plan owners can view suitable candidates to include in the succession plan.

Before you start

First, your organization needs to ensure that these tasks are completed:

- Migrate to Enhanced Talent Profiles.
- Set up job model profiles and person profiles. Associate job model profiles with jobs.
- Set up position profiles. Associate position profiles with job model profiles.
- Employees need to complete their talent profiles.
- Associate employees with a job that has a well-defined job model profile.
- Activate AI apps and ingest data.
- Activate AI Talent Best Match feature.

Configure Profile Options

You need to configure profile options related to the Suggested Successor feature to view AI based candidate suggestions. Use the **Manage Administrator Profile Values** task in the Setup and Maintenance work area to configure the values of the profile options listed in this table.

Profile Option Code	Profile Option Name	Value to Set	Effect of Enabling
ORA_HRM_ENABLE_AI_CANDIDATE_RECOMMENDATIONS	AI-Suggested Candidate Enabled	Y	Users can add AI suggested candidates to succession plans.
ORA_HRM_AI_CANDIDATE_RECOMMENDATIONS_LIMIT	Maximum Number of AI-Suggested Candidates to Show	A number less than 50	The number of candidate suggestions shown to users corresponds to the value specified. **Note:** The default value is **5**.

8 Extend Succession Management pages

Use the Express mode in Visual Builder Studio to control the fields, regions, and features of Redwood Succession Management pages that are available to your users.

This table lists the page properties that you need to enable for various features in Redwood Succession Management.

Page Property Name	Page	Effect of Enabling
Show the View Succession Organization Chart Button on the Succession Plan Overview Page	Succession Overview	HR specialists can use the **View Succession Organization Chart** button to view the succession organization chart of a person.
Show View External Candidates Button on the Succession Overview Page	Succession Overview	HR specialists can use the **View External Candidates** button to view external candidates to add to succession plans.
Show View Plan History Action on the Succession Overview Page	Succession Overview	HR specialists can use the **View Plan History** action to view the history of changes of a succession plan.
Set Color Codes for Readiness Categories of Candidates	Succession Overview	HR specialists can configure colors for specific readiness categories of succession plan candidates.
Control Default Filters and Display Order on the Succession Overview Page	Succession Overview	Determine the filters that HR specialists can see and the order in which these filters appear.
Show View Plan History Button on the Edit Succession Plan Page	Edit Succession Plan	HR specialists can use the **View Plan History** button to view the history of changes of a succession plan.
Show Add to Talent Pool Button	Edit Succession Plan	HR specialists can add selected candidates to talent pools.
Hide Candidate Selection Checkbox	Edit Succession Plan	HR specialists can't select candidates in the Candidates section when editing a succession plan.
Show Add Using Best-Fit Button for Plan Candidates	Edit Succession Plan	HR specialists can add candidates using the Best-Fit method.
Show View Incumbents Button	Edit Succession Plan, Create Succession Plan	HR specialists can use the **View Incumbents** button to view the incumbents of a Position or Job type succession plan.
Set Color Codes for Readiness Categories on Succession Organization Chart	Organization Chart	HR specialists can configure colors for specific readiness categories of succession plan candidates on the Succession Plans and Candidate in Plans tabs of a succession organization chart.
View Incumbents	Add to Succession Plan	HR specialists can use the **View Incumbents** button to view the incumbents of a Position or Job type succession plan.

Page Property Name	Page	Effect of Enabling
View Incumbents	Create Succession Plan	HR specialists can use the **View Incumbents** button to view the incumbents of a Position or Job type succession plan.