Oracle Fusion Cloud Human Resources

Oracle Search Cloud Service

Oracle Fusion Cloud Human Resources
Oracle Search Cloud Service

G42978-02

Author: Ashita Mathur

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

What's Oracle Search?

Oracle Search is a powerful search engine in HCM Cloud that can quickly search across large volumes of data and return highly relevant results.

Oracle Search-based searches provide a faster search experience and introduces these new search capabilities:

- Improved relevancy of results
- Ability to search based on keyword and faceted filtering with useful aggregation counts.
- Fuzzy matching
- Search on synonyms

Oracle Search enables powerful, index-based search functionality within Oracle cloud applications and is used to find information quickly and accurately across large volumes of data, improve search results in Redwood pages, and provide a better user experience for searching applications like Human Capital Management and Supply Chain Management. Oracle Search works by creating and managing search indexes and data security, which must be initially set up through a scheduled process before the search function is fully available.

Oracle Search in HCM and Other Fusion Applications

Oracle Search is widely used in HCM and the following modules are examples where Oracle Search powered features are used:

- Redwood quick actions person searches under My Team and My Client Groups tabs.
- Person Spotlight search page where the advanced search experience is designed for HR professionals.
- Redwood work structures management pages, including locations, departments, positions, and jobs.
- Inline person search LOVs embedded in transactional pages including workers list of values.
- Inline work structures LOVs embedded in transactional pages for locations, positions, jobs, and departments lists of values.
- Journeys.
- And others.

Other pillars, such as SCM also use Oracle Search. To learn more, go to the *SCM documentation:*

> **Note:** Oracle Search is required for Redwood enablement in HCM because all person searches in Redwood depend on Oracle Search-based person searches.

2 Initial Setup of Oracle Search

Set Up Oracle Search

You need to configure profile options and run the initial data ingestion process to set up the Oracle Search index, which is the foundation of Oracle Search based Global Search.

You have to do the following to set up Oracle Search:

- *Enable Oracle Search Profile Options*
- *Run Initial Data Ingestion*
- *Refresh Indexes After Upgrade*
- *Refresh Indexes After P2T*

Enable Oracle Search Profile Options

1. Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
2. Search for and review the following profile options. Set the values with the corresponding level if not set already.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_FND_SEARCH_EXT_ENABLED	Enable/Disable Search Ext Framework	Oracle Middleware Extensions for Applications	Oracle Middleware Extensions for Applications	Site	Yes
HRC_ELASTIC_SEARCH_ENABLED	HRC: Enable Elastic Search	HCM Common Architecture	Search Framework	Site	Y
PER_SEARCH_LOGIN_EVENT_PUB	PER: User Login Event Publication for Search	Global Human Resources	Security	Site	ATOM

Run Initial Data Ingestion

What's Initial Ingestion

A search index is a structured data store that enables fast and relevant search. Index allows the search engine to quickly look up documents that match a query.

The initial ingestion process is how the content becomes searchable in Oracle Search. It includes populating the searchable data from the relational database into the search index. Once ingested into the index, the content becomes then available for search engine.

The very first ingestion of searchable data into the search index is called the initial data ingestion. Initial ingestion of each search index utilized should only be done manually, once at initial configuration, and never scheduled.

If you're setting up multiple indexes for HCM products, then you must submit the process in a sequence with each index name as input parameter in serial. We recommend you submit indexes one by one to keep from loading up the Oracle Search Cloud Service (OSCS).

Run the Initial Data Ingestion

You must now run the initial data ingestion.

1. Navigate to **Tools > Scheduled Processes**.
2. Select **ESS job to create index definition and perform initial ingest to OSCS** from the menu and click **OK**.

   > **Note:** If you need to set up the index for a feature, select the relevant parameter value. For example, fa-hcm-person for person search or fa-hcm-position for positions search. If you're setting up multiple indexes, then you need to run multiple processes with different index name parameters.

3. Enter the index you want to ingest in the **Index Name to Reingest** field. For example:
   - Enter fa-hcm-person for the person index.
   - If you're setting up multiple indexes for HCM products, then you must submit the process in a sequence with each index name as input parameter in serial. We recommended you submit indexes one by one to keep from loading up the Oracle Search Cloud Service (OSCS).
   - This process is secured with FND_MANAGE_SCHEDULED_JOB_DEFINITION_PRIV function privilege. The privilege is available in the ORA_FND_APPLICATION_ADMINISTRATOR_JOB or ORA_FND_APPLICATION_DEVELOPER_JOB job roles.
4. Launch the process for each HCM product deployed in your environment.

Product	Index name
General search infrastructure	- fa-hcm-savedsearch
Global Human Resources	- fa-hcm-person - fa-hcm-job - fa-hcm-position - fa-hcm-location - fa-hcm-organization
Learning	- fa-hcm-learningitem - fa-hcm-learn-acl - fa-hcm-learningrecord - fa-hcm-learningbooking - fa-hcm-wlf-recommendationprofile - fa-hcm-wlf-recommendation

Product	Index name
Time and Labor	o fa-hcm-timecard
Recruiting	o fa-hcm-requisition o fa-hcm-irc-hiring-events o fa-hcm-irc-messages
Career and Profile Management	o fa-hcm-modelprofile o fa-hcm-personprofile
Journeys	o fa-hcm-workerjourney o fa-hcm-workerjourneytask
Connections	o fa-hcm-profile-tag
Benefits	o fa-hcm-person benefits
Profile Management	o fa-hcm-contentitem o fa-hcm-teamskills

Refresh Indexes After Upgrade

Oracle Search indexes are automatically reingested with release upgrades. You must not reingest the existing Oracle Search indexes manually.

The automated reingestion will only reingest if new attributes are added to an index. Automated ingestion process is nondestructive and runs in the background while existing indexes are available.

Related Topics

- Set Profile Option Values
- Submit Scheduled Processes and Process Sets

Refresh Indexes After P2T

You need to do the following:

- Run the initial data ingestion process manually for every created index after P2T (production-to-test) process.
- Run the Compute Users ACL process with User Population = All Users after P2T (production-to-test) process.

Note: As a best practice, review your P2T checklist and add this step to the checklist. It should also include the list of all indices that you have to reingest during the P2T process. If you don't have the P2T checklist, consider creating such a checklist, including the steps that you have to do after each P2T, as this will streamline your p2T processing moving forward and help to avoid mistakes.

For more information refer to the post P2T doc - *Oracle Applications Cloud Service Definition - Environment Refresh (Doc ID 2015788.1)*

Information about pre and post P2T steps can be found in Appendix D: APPENDIX D: PREPARING AND ADJUSTING YOUR ENVIRONMENTS BEFORE AND AFTER ENVIRONMENT REFRESH

Set Up Oracle Search for List of Values

You can set up Oracle Search for these List Of Values (LOVs).

- *Oracle Search for Workers List of Values*
- *Oracle Search for Positions List of Values*
- *Oracle Search for Departments List of Values*
- *Oracle Search for Locations List of Values*
- *Oracle Search for Jobs List of Values*

Oracle Search for Workers List of Values

Here are the steps to enable Oracle Search for workers list of values:

1. Create the person index, fa-hcm-person and set up Oracle Search. For details, see *Set Up Oracle Search*.
2. Set up data security for Oracle Search. For details, see *Set Up Data Security for Oracle Search*.
3. Enable Oracle Search for workers LOV:
    - Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
    - Search and set these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_PER_ ORACLE_SEARCH_ WORKERSLOV_ ENABLED	Enable Oracle Search Workers Lov	Global Human Resources	Personal Information	Site	Yes

Note: Oracle Search based public person search doesn't implement the public person security profile, it always returns all results, by default. You can use the Public Worker Access configuration to set up the restricted public person search policy with Oracle Search. For more information on how to review the following*Set Up Public Worker Access* Private person security profile is fully implemented with Oracle Search.

Oracle Search for Positions List of Values

Here are the steps to enable Oracle Search for positions list of values:

1. Create the position index, fa-hcm-position and set up Oracle Search. For details, see *Set Up Oracle Search*.
2. Set up data security for Oracle Search. For details, see *Set Up Data Security for Oracle Search*.
3. Enable Oracle Search for positions LOV using these steps:
    - Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
    - Search and set these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_PER_ORACLE_SEARCH_POSITIONSLOV_ENABLED	Enable Oracle Search for Positions Lov	Global Human Resources	Personal Information	Site	Y

Oracle Search for Departments List of Values

Here are the steps to enable Oracle Search for departments list of values:

1. Create the departments index, fa-hcm-organization and set up Oracle Search. For details, see *Set Up Oracle Search*.
2. Set up data security for Oracle Search. For details, see *Set Up Data Security for Oracle Search*.
3. Enable Oracle Search for departments LOV using these steps:
    - Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
    - Search and set these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_PER_ORACLE_SEARCH_DEPARTMENTSLOV_ENABLED	Enable Oracle Search for Departments Lov	Global Human Resources	Personal Information	Site	Y

Oracle Search for Locations List of Values

1. Create the locations index, fa-hcm-location and set up Oracle Search. For details, see *Set Up Oracle Search*.
2. Set up data security for Oracle Search. For details, see *Set Up Data Security for Oracle Search*.
3. Enable Oracle Search for locations LOV using these steps:

- Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
- Search and set these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_PER_ORACLE_SEARCH_LOCATIONSLOV_ENABLED	Enable Oracle Search for Locations Lov	Global Human Resources	Personal Information	Site	Y

Oracle Search for Jobs List of Values

1. Create the jobs index, fa-hcm-job and set up Oracle Search. For details, see *Set Up Oracle Search*.
2. Set up data security for Oracle Search. For details, see *Set Up Data Security for Oracle Search*.
3. Enable Oracle Search for jobs LOV using these steps:
   - Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.
   - Search and set these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
ORA_PER_ORACLE_SEARCH_JOBSLOV_ENABLED	Enable Oracle Search for Jobs Lov	Global Human Resources	Personal Information	Site	Y

Set Up Data Security for Oracle Search

Next, you need to set up Oracle Search data security with dynamically computed access control lists (ACLs).

As part of setting up data security for Oracle Search, you have to do the following:

- *Enable Logging Profile Options*
- *Initiate ACL Ingestion*
- *Schedule ACL Processes*

Enable Logging Profile Options

You need to run Access Control List (ACL) processes with some minimum logging capabilities. Enable these profile options:

1. Navigate to **Home > Setup and Maintenance > Manage Administrator Profile Values**.

2. Search and enable these profile options.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
AFLOG_ENABLED	FND: Log Enabled	Oracle Middleware Extensions for Applications	Application Logging	Site or User level for the user running ACL processes	Yes
AFLOG_LEVEL	FND: Log Level	HCM Common Architecture	Application Logging	Site or User level for the user running ACL processes	Severe
AFLOG_MODULE	FND: Log Module Filter	Global Human Resources	Application Logging	Site or User level for the user running ACL processes	%

Initiate ACL Ingestion

An ACL (Access Control List) in Oracle Search defines which users are allowed to see specific search results.

During search, Oracle Search automatically filters results based on these ACLs so users only see items they are authorized to access - such as their own assignments, workers in their hierarchy, or data allowed by their job roles and privileges. The Access Control Lists must be computed in order to properly store the detailed information which records user is authorized to access.

HCM Access Control List initial ingestion is a process which creates the required ACL index, computes the ACL for each user in the system and validates the ACL index to ensure stability.

Run this only once at initial configuration. If you have already implemented Oracle Search, there is no need to run this process again.

Note: Do this step only once when setting up data security for Oracle Search with the first implementation.

1. Navigate to **Tools > Scheduled Processes**.
2. Run the process that's described in this table.

Job Name	Description
HCM Access Control List Initial Ingestion	Creates HCM access control list and performs the initial ingestion.

Note:

- This process should not be run periodically and should not be scheduled.
- Running this process isn't required with release upgrades.

Schedule ACL Processes

Schedule these ACL (access control list) processes, if they're not yet scheduled.

1. Navigate to **Tools > Scheduled Processes**.
2. Schedule these processes.

Job Name			**Frequency**
Compute Users ACL by Event			Every 15-60 minutes
Job Name	**Parameter Name**	**Parameter Value**	**Frequency**
Compute Users ACL	User Population	Logged in users	Every 30-120 minutes
Compute Users with Large ACL	Action	Compute	Daily
	User Population	All users with Large ACL	

Note:

- The process Compute Users ACL with parameter User Population = All users should not be run periodically and should not be scheduled.
- The process Compute Users ACL with parameter User Population = All Users after P2T (production-to-test) process..

Set Up Public Worker Access

You can configure access for public workers using the Configure Public Workers Access page under Workforce Structures under My Client Groups tab.

This page can now be used to determine which public workers are returned when using Oracle Search. For example, when using Connections, you're initially prompted for the person's name whose information you're looking for. By configuring Public Worker Access, you can now create a filter that lets you to hide sensitive or non-public workers by user-defined criteria, such as job code, position, business units, and other criteria. This filter is also applied to the global search and public worker LOVs that use Oracle Search, including Human Capital Management, Procurement, Supply Chain Management, and so on.

You can restrict Public Worker Access based on these scenarios.

1. All workers in the enterprise, but exclude certain people based on criteria;
2. Workers from the user's own legal employer;
3. Workers from the user's own business unit; and
4. Workers based on other inclusion criteria.

By default, Status is a read-only field and is determined based on the Enable Public Worker Access Using Security Filters Enabled profile option. If the profile option is disabled, filtering won't happen and you'll see all workers.

When selecting which workers to include you can also specify the users you want to exclude. For example, when selecting workers from the user's legal employer, you can exclude people from a business unit.

With the **Workers in a user's legal employer** option, you can configure multiple criteria and values to exclude, except for legal employer. An error appears if you choose a legal employer as this choice conflicts with the public workers inclusion selection.

With the **Workers in a user's business unit** option, you can configure multiple criteria and values to exclude, except for business unit. An error appears if you choose Business unit as this choice conflicts with the public workers inclusion selection.

Public workers LOV will list all workers in the signed-in user's business units that aren't in a grade of EXTS_GRADE, aren't in CEO or CFO jobs, and aren't consultants or pending workers. Additionally, Larry Benson is identified as a sensitive person, so he will also be filtered out.

With the **Other inclusion criteria option**, you can configure multiple criteria and values to include and exclude.

Access

To use this feature, you need this job role name and code:

- **IT Security Manager (ORA_FND_IT_SECURITY_MANAGER_JOB)**

If you've created a custom IT Security Manager job role, then you'll need to add the **Configure Public Worker Access** function privilege.

Enable Global Search

Global Search in Oracle Fusion Applications is a unified, application-wide search feature that lets users quickly find data, pages, and actions across all modules (HCM, Finance, SCM, CX, and so on.) from a single search bar.

Behind the scenes, Global Search uses the Oracle Search as a search method.

You need to configure the Global Search profile option and review the configuration for HCM to enable Global Search with Oracle Search capabilities.

Typically the Global Search enabled with Oracle Search requires the following:

- *Create Person Index*
- *Enable Global Search Profile Option*
- *Review Global Search Configuration for HCM*

Create Person Index

This feature requires an Oracle Search index. Ensure that the required index, fa-hcm-person is created and data is ingested. Follow the steps listed in *Set Up Oracle Search*.

If person search for Oracle Search has already been implemented, you don't need to implement it again.

Note: Oracle Search based public person search doesn't implement the public person security profile, it always returns all results, by default. You can use the Public Worker Access configuration to set up the restricted public person search policy with Oracle Search. For more information on how to *Set Up Public Worker Access* check the above topic: Private person security profile is fully implemented with Oracle Search.

Enable Global Search Profile Option

1. Navigateeto **Home > Setup and Maintenance > Manage Global Search Profile Options**.
2. Search and set this profile option.

Profile Option Code	Profile Display Name	Application	Module	Profile Level	Profile Value
FUSION_APPS_ SEARCH_ENABLED	Global Search Enabled	Oracle Middleware Extensions for Applications	Oracle Middleware Extensions for Applications	Site	Yes

Review Global Search Configuration for HCM

1. Navigate to **Home > Setup and Maintenance > Manage Global Search Configurations**.
2. Ensure that global search is configured and enabled for HCM.
3. Ensure that the following **Suggestion Group** is enabled in the Global Search Configuration for HCM.

Short Name	Display Name	Description
HCM_PERSON_SEARCH	Oracle HCM Cloud Global Search for Person Action	This is the Global Search for HCM Person.

3 Setup Additional HCM Module Implementations

Best Practices for Setting Up Additional HCM Module Implementations with Oracle Search

Follow these best practices when setting up additional HCM module implementations with Oracle Search.

- Run the initial data ingestion (ESS job to ingest) only for the new index that's required by the new module.
- Run the Compute Users ACL with parameter population = All users, only after all functional indices required by your implementation were ingested.
  - This job will not cause any downtime for users working with already implemented Oracle Searches.
- Do not run the HCM Access Control List Initial Ingestion job. Running this job after you implemented some searches will cause users search downtime until it's completed because it's re-creating the ACL index from scratch.

Enable the module specific profile options if needed. Review your module documentation for details.

HCM Module Specific Oracle Search Resources

This topic includes documentation links for all products in HCM that use OS including additional product configuration:

- Learning
  - *Prepare Oracle Learning for Redwood*
- Time and Labor
  - *fa-hcm-timecard*
- Recruiting
  - *Prepare Recruiting for Redwood*
  - fa-hcm-requisition
  - fa-hcm-irc-hiring-events
  - fa-hcm-irc-messages
- Career and Profile Management
  - fa-hcm-modelprofile
  - fa-hcm-personprofile
- Journeys
  - fa-hcm-workerjourney
  - fa-hcm-workerjourneytask
- Connections
  - fa-hcm-profile-tag

- Benefits
  - *fa-hcm-person benefits*

4 Search Experience Configuration

Search Experience Configuration

You can configure the search experience on selected pages using the Search Views. You can access the Search Views admin page using the quick action under **My Client Groups > Data Exchange**.

With Search Views, you can set up the following:

- Enable the default search results on the page load
- Define the keyword search fields
- Enable available search filters
- Display and hide the default result columns
- Set up available sorting options

Native fields are supported and on selected search pages also custom fields are configurable as search fields, filters or result columns, or both.

> **Note:** If you want to configure custom fields in your search experience, the custom fields must be added to the corresponding index first.

Review the following documentation for more details:

- *https://docs.oracle.com/en/cloud/saas/applications-common/25d/facia/add-extensible-attributes-to-search-indexes.html*
- *https://docs.oracle.com/en/cloud/saas/applications-common/25d/facia/remove-extensible-attributes-from-search-indexes.html*

Best Practices for Search Experience Configuration

- Don't enable too many search fields. Search results are optimal when up to 4-5 search fields are configured.
- Don't enable too many extensible attributes in the search index as it impacts the overall index size and search performance.
  - Use only the minimum required number of extensible attributes to enhance your search experience.
  - Don't enable extensible attributes in the search index that may not be used with the pages offering search experience.

5 Implementing Oracle Search - Do's and Don'ts

Implementing Oracle Search - Do's and Don'ts

Do's	Don'ts
Run the 'Compute Users ACL with parameter User Population = All Users' ESS job only ONCE after the new module(s) have been ingested for additional product implementation in OS.	DO NOT re-run the Initiate ACL Ingestion job set for any additional product OS implementations. This is done only once at initial implementation. This is a job set which creates empty ACL index first and follows with the computation of ACL for all users. This may cause users of existing implementation not being able to view results in secured searches until this job is completed. • DO NOT schedule the 'Compute Users ACL with parameter User Population = All Users', as this could cause performance issues.
Review if the ACL refresh jobs are scheduled on your application. This is important to ensure searches apply the up-to-date data security policies.	The process Compute Users ACL with parameter User Population = All users should not be run periodically and should not be scheduled.
Review if the ACL refresh jobs are scheduled on your application. This is important to ensure searches apply the up-to-date data security policies.	Don't schedule the ingestion of functional indices. It's not necessary and will only consume system resources.
Run periodical health checks of functional index ingestions with diagnostic reports to identify ingestion issues. There are *reports* for person, journeys, work structures, and so on. • Run Compute Users ACL with population = All Users after P2T (on the target environment).	Don't run initial ingestion of functional indices (such as fa-hcm-person or fa-hcm-position) as part of the release upgrade. There is an automated ingestion process implemented, which will re-ingest indices that require full re-ingestion upon release upgrade.

Best Practices for Scenario-based Use Cases

Case	Key Points	ACL process to run	ACL Frequency	When to run
Update of a security role where majority of users are impacted	If a role that impacts majority of the population like employee or line manager role has been modified and some new privileges have been added or removed, execute ACL process for all users	Stop Business As Usual Incremental jobs.) Compute Users ACL (Parameter - All Users) ,	Once	To be run in off business hours or cut-off period
Update of a security role where only a handful of users are impacted	If a role impacting a handful of population like an admin role has been modified for which only a	Individual ACLs can be computed for a user using the Regenerate ACL action	Once per user	Can be run during business hours

Case	Key Points	ACL process to run	ACL Frequency	When to run
	small population of support and admin users have been assigned.	available in the "Preview HCM Data Security."		
Major re-org within enterprise. (including mergers and acquisitions).	Execute the ACL process for all users. ACL index will be updated, and it will be run for all users.	Pause the incremental schedule, run Compute Users ACL (Parameter - All Users) only once, and then resume the incremental schedule.	Once	To be run in off business hours or cut-off period

6 Oracle Search Maintenance

Oracle Search Maintenance

- Refresh Indexes After Upgrade

Oracle Search indexes are automatically reingested with release upgrades. You must not reingest the existing Oracle Search indexes manually.

The automated reingestion will only reingest if new attributes are added to an index. Automated ingestion process is non-destructive and runs in the background while existing indexes are available.

- Refresh Indexes After P2T

You need to run the initial data ingestion process manually for every created index after P2T (production-to-test) process.

Run the Compute Users ACL process with User Population = All Users after P2T (production-to-test) process.

> **Note:** As a best practice, review your P2T checklist and add this step to the checklist. It should also include the list of all indices that you have to reingest during the P2T process. If you don't have the P2T checklist, consider creating such a checklist, including the steps that you have to do after each P2T, as this will streamline your p2T processing moving forward and help to avoid mistakes.

- Maintaining Oracle Search for Oracle Recruiting
  - *Maintaining Oracle Search for Oracle Recruiting*

7 Troubleshooting

Oracle Search Diagnostics

Users can search for other people, actions, jobs, locations, positions, and so on using Oracle Search but can occasionally run into problems.

- The following diagnostics are available to assist in getting these issues resolved:
  - HCM Oracle Search Person Index Diagnostic Report
  - HCM Oracle Search Job Index Diagnostic Report
  - HCM Oracle Search Location Index Diagnostic Report
  - HCM Oracle Search Model Profile Index Diagnostic Report
  - HCM Oracle Search Organization Index Diagnostic Report
  - HCM Oracle Search Person Profile Index Diagnostic Report
  - HCM Oracle Search Position Index Diagnostic Report
  - *HCM Journeys Oracle Search Diagnostics Report*
  - HCM Benefits Search Person Index Diagnostic Report

For information on how to find and run the diagnostic go to *Run Diagnostic Tests*

> **Note:** Diagnostic reports compare the number of records in database and in Oracle Search. The top-level object counts should match. If you identify a minor mismatch, review the ingestion logs to identify potentially not ingested records and then work with support to add these individual records to the index.

Best Practices

Search Behavior	More Info Needed	Best Practice
Search not returning any results	Does it happen to all users?	• Review the functional index health (diagnostic report). • Review ACL index exists and computation has been completed for all users.
	Does it happen to single user only?	• Review user's ACL and regenerate if needed. • Review user's access to search APIs.
Search not returning only selected records, most of results returned as expected.	n/a	• Verify missing record with diagnostic report (for example, provide person number in the diagnostic report and

Search Behavior	More Info Needed	Best Practice
		review the results). If record is missing in the functional index, work with support to ingest missing record. • Use the hcm data security preview page and verify if the user has access to record being searched. • Regenerate user's ACL if needed.