# Oracle Fusion Cloud Customer Experience

## What are the basic security concepts and procedures for Oracle CX?

Oracle Fusion Cloud Customer Experience
What are the basic security concepts and procedures for Oracle CX?

G30353-04

*Copyright* © 2025, Oracle and/or its affiliates.

Author: Carmen Myrick

# 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*.

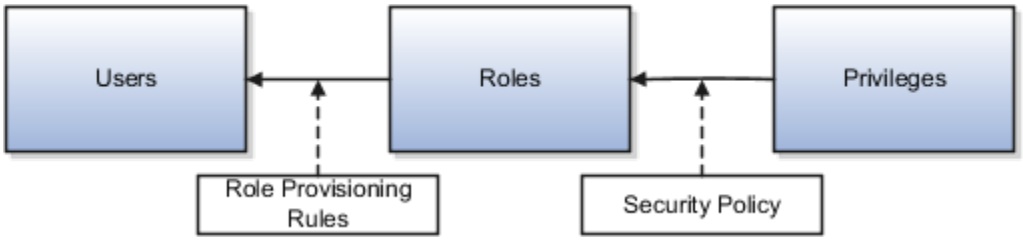
Thanks for helping us improve our user assistance!

# 1 Introduction

## Overview of Role-Based Access Control (RBAC)

Oracle Fusion applications use a role-based access control (RBAC) security model to secure access to functionality and data. With RBAC, you provide users with roles, and the roles are assigned access privileges.

This diagram shows the relationship between users, roles, and privileges. Users get roles assigned. The roles contain privileges to access functionality and data.




In Oracle CX, users gain access to application data and functions when you assign them these types of roles:

- Job roles: These give users the permissions they need to perform tasks that are specific to a job, such as a salesperson or sales manager.
- Abstract roles: These give users the permissions to complete tasks that are common to all users.

Users can have any number of different roles at the same time. The combination of roles determines the user's level of access to protected system resources. For example, a user might be assigned the Sales Manager role, the Sales Analyst role, and the Employee role. In this case, the user has this access:

- As an employee, the user can access employee functions and data.
- As a sales manager, the user can access sales manager functions and data.
- As a sales analyst, the user can access sales analysis functions and data.

When the user signs in to the application and is successfully authenticated, a user session is established. All the roles assigned to the user are loaded into the session repository. The application determines the set of privileges for application resources that are provided by the roles and then grants the user the most permissive level of access.

You can assign roles to a user manually when you create the user, or automatically, by creating role provisioning rules.

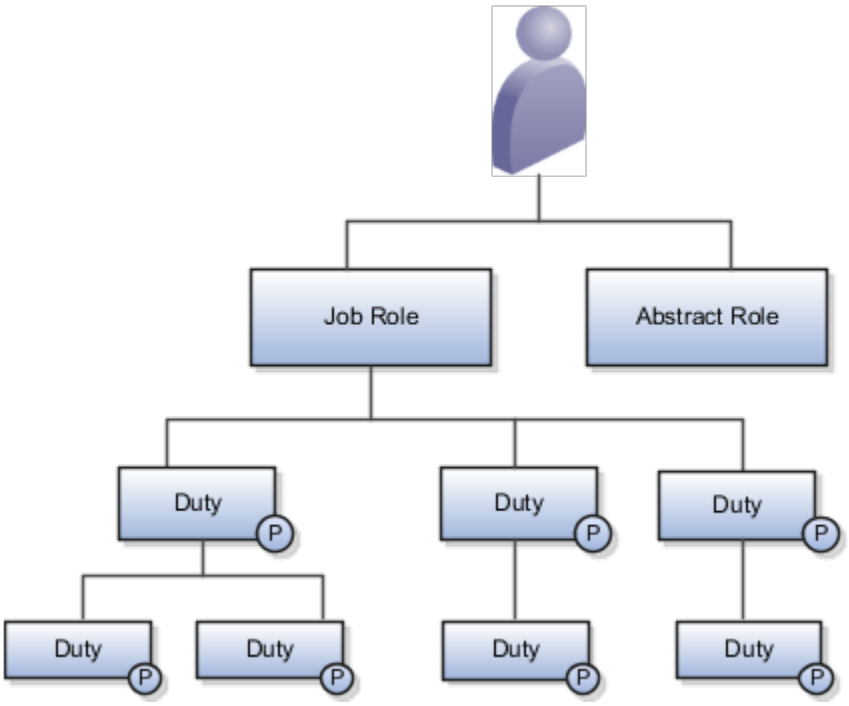
*Related Topics*

- Role Provisioning

## Role Hierarchies and Role Inheritance

Each role is a hierarchy of other roles that are linked to each other in a parent-child relationship. As this hierarchy chart shows, users are assigned job and abstract roles, which inherit duty roles and their associated privileges.

Duty roles in turn can inherit privileges from subordinate duty roles. You can explore the complete structure of a job or abstract role on the Security Console.

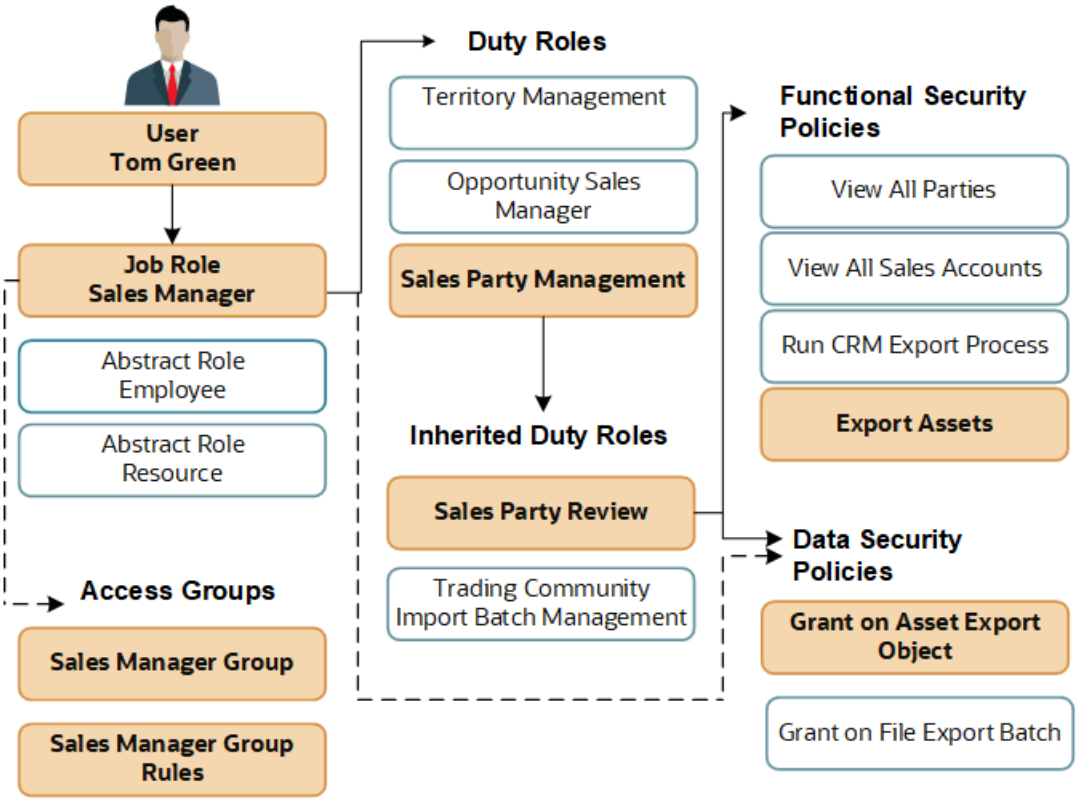



Role hierarchies allow privileges to be grouped to represent a feature set, which simplifies feature management. Role hierarchies also provide privilege granularity and facilitate role reuse. For example, each role hierarchy beneath the job role represents a feature that's available through the job role to the user. Roles at lower levels of the hierarchy represent functionality that the feature requires. If this functionality is required by other features, the role that provides the functionality can be shared across roles.

**Note:** Having many levels in a role hierarchy isn't recommended. Deep role hierarchies are difficult to manage, and modification of the privileges in roles that are heavily reused can cause undesired consequences in other features.

## Role Inheritance Example

This example shows how roles and privileges are inherited for a user, Tom Green, assigned the Sales Manager job role. The chart shows a few of the duty roles that Tom inherits.




As an employee sales manager, Tom Green is provisioned with the roles required to do the job: the Sales Manager job role, and the Employee and Resource abstract roles. Roles are inherited like this:

- The Sales Manager job role inherits duty roles including the Sales Party Management duty role and the Opportunity Sales Manager duty role.
- Duty roles inherit other duty roles. For example, the Sales Party Management duty inherits the Sales Party Review duty and the Trading Community Import Batch Management duty, as well as many privileges.
- The duty roles can be associated with functional security policies and data security policies. For example, the inherited Sales Party Review duty includes security policies that specify which application pages sales managers can access to export assets.
- Data security policies are also assigned to the Sales Manager job role directly.
- When the sales manager Tom Green is provisioned with the Sales Manager job role, he's also automatically enrolled into a system access group, the Sales Manager Group, which is assigned rules that provide the same access to data as the data security policies assigned to the Sales Manager job role.

  If you were provisioned with the sales application for the first time in Update 22B or later, your database resources are secured using system access groups and rules by default. Using access groups and rules is also the recommended way of configuring data security. For more information about access groups, see *Overview of Access Groups*.

# Predefined Sales and Service Roles

Oracle provides many predefined job and abstract roles as part of the security reference implementation for Sales and Fusion Service. The security reference implementation is a predefined set of security definitions that you can use as-is.

## Sales Roles

Here are some of the predefined job roles for sales users:

- Channel Account Manager
- Channel Operations Manager
- Channel Sales Manager
- Customer Contract Administrator
- Customer Data Steward
- Customer Relationship Management Application Administrator
- Data Steward Manager
- Enterprise Contract Administrator
- Enterprise Contract Manager
- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst
- Inside Sales Manager
- Inside Sales Representative
- Marketing Manager
- Marketing Operations Manager
- Marketing VP
- Master Data Management Application Administrator
- Partner Administrator
- Partner Sales Manager
- Partner Sales Representative
- Sales Administrator
- Sales Analyst
- Sales Catalog Administrator
- Sales Lead Qualifier
- Sales Manager
- Sales Representative
- Sales VP
- Supplier Contract Administrator

You also assign the following abstract roles to sales users who are employees so they can carry out their work:

- Employee
- Resource

**Note:** Be extremely cautious when assigning predefined roles as-is. See *Guidance for Assigning Predefined Roles* and *Advisory Note on Subscription Impact*.

If you're using the Incentive Compensation functionality, you can also assign the following abstract roles to users:

- Incentive Compensation Participant
- Incentive Compensation Participant Manager

## Service Roles

Several job roles and duty roles are predefined in the Service offering. These are the predefined job roles specific to this product area:

- Chat Agent
- Customer Service Manager
- Customer Service Representative
- Knowledge Analyst
- Knowledge Manager
- Field Service Technician
- Internal Help Desk Administrator
- Internal Help Desk Agent
- Internal Help Desk Manager
- Case Manager
- Case Worker

# Options for Reviewing Predefined Roles

There are many ways to access information about predefined roles. You can use the Security Console or the Sales and Service Access Management Work Area. There are user reports. And, you can consult the security reference manuals.

**Note:** For best practices around assigning predefined roles, see *Guidance for Assigning Predefined Roles*.

## Security Console

Let's briefly review the Oracle Applications Cloud Security Console. On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.

- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

**Tip:** Predefined roles have the code prefix `ORA_`.

For more information about the Security Console, see *Overview of Security Console*.

## User and Role Reports

You can run the User and Role Access Audit Report to produce an XML-format report of the function security privileges and data security policies for a specified role, all roles, a specified user, or all users.

Also see: *What user reports are there?*

## Security Reference Manuals

These guides describe the security reference implementation for Oracle Sales and Fusion Service users:

- *Security Reference for Sales and Fusion Service*
- *Security Reference for Enterprise Contracts*
- *Security Reference for Incentive Compensation*
- *Security Reference for Common Features*

These guides contain a section for each predefined job and abstract role. For each role, you can review:

- Duty roles
- Role hierarchy
- Function security privileges
- Data security policies

You can access the security reference manuals on *Oracle Help Center*.

## Sales and Service Access Management Work Area

You can review the visibility provided by a job role to object data in the Sales and Service Access Management work area. You can display a read-only view of all the data security policies provided by a selected role for a selected object.

Also see *Security Configuration Work Areas*

# Roles for Workflow Administration Access

Predefined roles provide access to workflow administration functionality. Users with the workflow roles can perform tasks such as setting up approval rules and managing submitted approval tasks.

This table lists the predefined Oracle Business Process Management (BPM) role for Sales workflow administration access and the predefined job roles that inherit it. It also shows the BPM role that provides workflow administration access for all product families. You can assign a predefined BPM role to a custom job role, if needed.

***Predefined Oracle Business Process Management (BPM) Roles***

| Product Family | Role Name and Code | Inherited by Job Role |
|---|---|---|
| Sales | BPM Workflow Customer Relationship Management Administrator<br><br>BPMWorkflowCRMAdmin | Corporate Marketing Manager<br><br>Customer Relationship Management Application Administrator<br><br>Marketing Analyst<br><br>Marketing Manager<br><br>Marketing Operations Manager<br><br>Marketing VP<br><br>Sales Lead Qualifier |
| All | BPM Workflow All Domains Administrator Role<br><br>BPMWorkflowAllDomainsAdmin | This role isn't assigned to any predefined job role, but you can add it to custom job roles. |

*Related Topics*

- Roles That Give Workflow Administrators Access

# Duty Roles

You may want to configure the predefined security model by creating your own duty roles. In this case, it's important to understand how duty roles are constructed.

A typical duty role consists of two components: data security policies, and function security privileges. Duty roles can also inherit other duty roles.

## Function Security Policies

Function security policies let a user who's assigned a duty role access different UI elements, web services, tasks flows, and other functions. For example, a sales manager who has the Delete Opportunity function security policy can view and click the Delete button. Removing that policy removes the button from view. A function security policy is composed of:

- A duty role name. The name of the duty where the policy applies, for example, Opportunity Sales Manager.
- A functional privilege that specifies the application features that are being secured, for example, Delete Opportunity.

Some UIs aren't subject to data security, so some function security privileges don't have an equal data security policy.

In the security reference manuals, functional privileges are listed in the Privileges section.

## Data Security Policies

Data security policies specify the roles that can perform a specified action on an object, and the conditions under which the action can be carried out. A data security policy is composed of:

- A role name. The name of the role the data security policy is granted to. The role can be a duty role, a job role or an abstract role. For example, the Opportunity Sales Manager duty role.
- The business object that's being accessed, for example, Opportunity. The data security policy identifies the object by its table name, for example, `MOO_OPTY` for opportunity.
- A data privilege that defines the actions allowed on the data. For example, View Opportunity.
- The condition that must be met for access to the business object to be granted. For example, sales managers can view opportunities as long as they're in the management chain or are members of the sales team for the opportunity.

  If the View All condition is specified, the role provides access to all data of the relevant type.

Data privileges are listed in the Data Security Policies section of the security reference manuals.

**Note:** You can use access groups to give sales resources additional access to sales object data

## Policy Store

The policy store is the repository of all roles for Oracle Cloud applications. The policy store is also where the security policies defined for each role are stored. The Security Console is a tool for managing the policy store for Oracle Cloud applications.

For more information, see *Duty Role Components*.

# Guidelines for Configuring Security

If the predefined security reference implementation doesn't fully represent your enterprise, then you can make changes.

For example, the predefined Sales Representative job role includes Sales Forecasting privileges. If sales managers do sales forecasting in your organization, not the salespeople, then you can create a salesperson role without those privileges. In this case, use the predefined Sales Representative role, or copy this role and make your own modifications. The role code of the Sales Representative application job role is `ORA_ZBS_SALES_REPRESENTATIVE_JOB`.

During implementation, you evaluate the predefined roles and decide whether changes are needed. If changes are required, then you can either create a role from scratch or copy an existing role. You can perform both tasks on the Security Console.

You can identify predefined roles easily by their role codes, which all have the prefix `ORA_`.

All predefined roles are granted several function security privileges and data security policies. They also inherit duty roles. To make minor changes to a role, copying the predefined role and editing the copy is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

## Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you can create your own job roles. Add duty roles to custom job roles, as appropriate.

## Predefined Roles with Different Privileges

If the privileges for a predefined job role don't match the corresponding job in your enterprise, then you can create your own version of the role. If you copy the predefined role, then you can edit the copy to add or remove duty roles, function security privileges, and data security policies, as necessary.

## Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you can create your own duty roles.

The typical implementation doesn't use custom duty roles.

*Related Topics*

- Options for Reviewing Predefined Roles

# 2 Data Sharing and Visibility

## Data Sharing Mechanisms

The conditions specified in access group rules or data security policies control visibility to record-level data associated with business objects like opportunities and leads.

Conditions can use the following components as mechanisms for sharing data, if the sharing mechanism is applicable for the object:

- Team
- Partner team
- Territory
- Resource hierarchy
- Business unit

For example, for the Opportunity object, data can be shared through team membership, through the resource hierarchy, or through territory membership.

## How Sales Users Gain Access to Sales Information

The security reference implementation provided by Oracle determines who can access opportunity information in your sales organization. While basic information on accounts and contacts is available to all salespeople, your access to sales data is restricted by your position in the resource hierarchy, membership in the sales team, and ownership.

Whether or not you can access a particular opportunity or a lead depends on your membership in the resource and territory hierarchies. Here's how you gain access to opportunities. Lead access follows the same pattern. You can access an opportunity if:

- You create the opportunity.
- You're on the opportunity sales team.
- The opportunity owner or sales team member is your direct or indirect report in the resource hierarchy.
- You're the owner or are a member of the territory assigned to the opportunity.
- You're the owner or member of a parent territory of the territory assigned to the opportunity.
- You're assigned to a territory for the account associated with the opportunity.
- You're assigned to a territory that's a parent of the territory for the account associated with the opportunity.

Salespeople can see all opportunities related to their accounts but access differs between territory members and opportunity members:

- An opportunity owner gets full access to the opportunity, which includes the ability to edit as well as add and remove team members.
- Owners and members of territories or parent territories assigned to the opportunity account get read-only access to the opportunity and aren't added to the opportunity sales team.

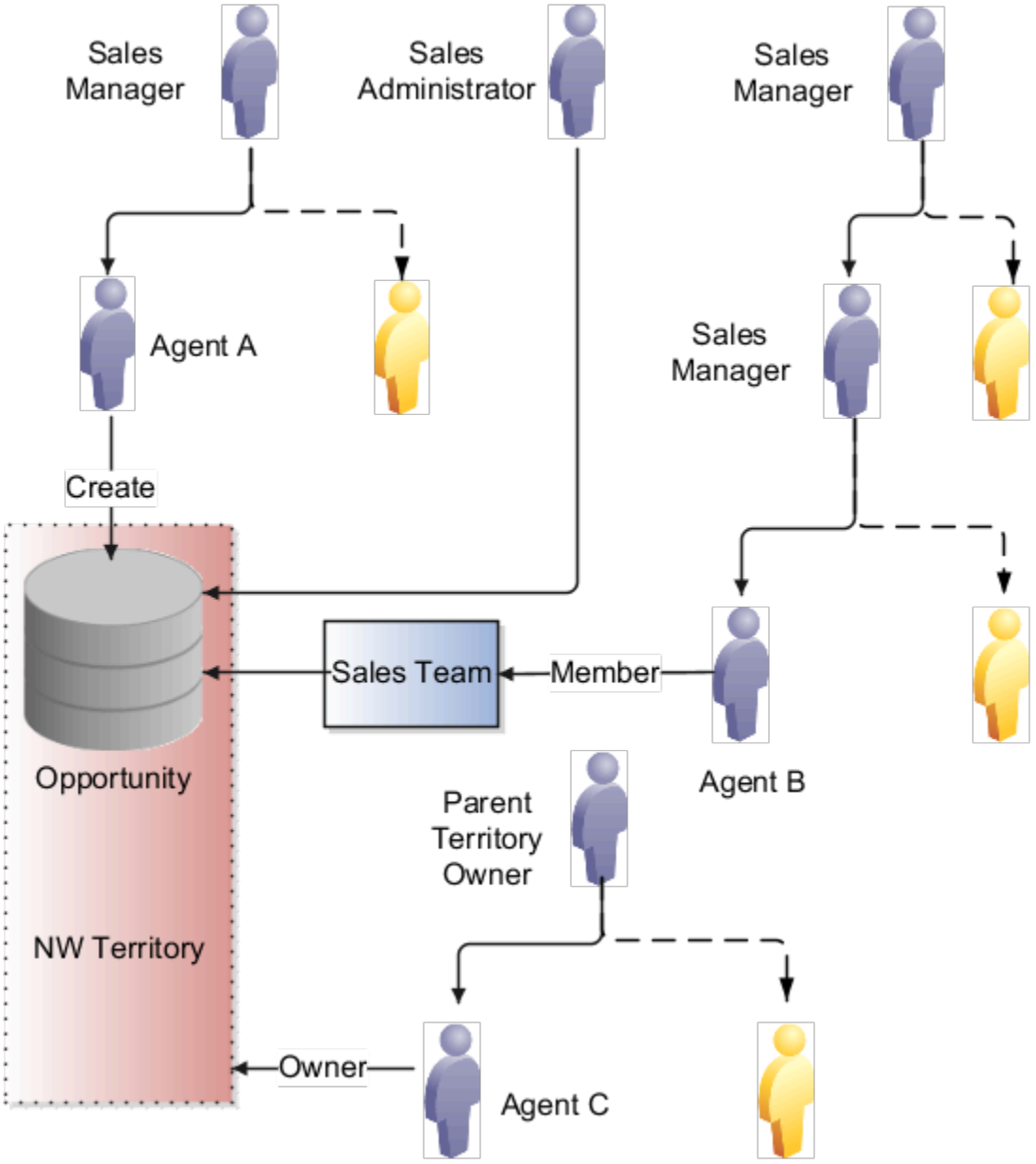
- Owners and members of territories assigned to the opportunity product lines are added as a distinct list of territories to the opportunity sales team. Owners and members of these territories get full access to the opportunity. Depending on a profile option, either only the owner or all the members of the territory are added as resources to the opportunity sales team. Regardless of the access level for these members as a resource on the opportunity team, they always have full access.

  Owners and members of parent territories of the territory assigned to the opportunity aren't added to the opportunity sales team but they always get full access.

The following diagram illustrates some of the different ways that you can gain access to an opportunity:

- Named agents in the diagram (A, B, and C) can access the opportunity.
- Unnamed agents (highlighted in yellow) can't access the opportunity.
- Sales managers can access the opportunity because a salesperson in their management chain has access.
- Owners of parent territories can access the opportunity through the sales territory hierarchy.

This diagram shows who in a sales hierarchy can access an opportunity.




- Agent A can access the opportunity because she created it. When you create an opportunity, you're the initial owner.
- Agent B can access the opportunity because he's on the sales team.
- Sales managers who are higher up in the management chain can also see the opportunity because access is provided through the resource hierarchy. The managers of Agent A and Agent B can access the opportunity information, but agent A and Agent B's colleagues can't.
- Agent C can access the opportunity because he's the owner of the NW territory. The owner of the parent territory can also access the opportunity.
- Sales administrators can access the opportunity.

**Note:** Access using accounts isn't shown in this diagram.

## Special Access

Some access isn't affected by the management hierarchy and membership in sales teams or territories. This special access includes:

- Administrators: Users assigned the Sales Administrator job role get full access to opportunities and other objects. This access is based on their privileges, regardless of where the administrators are in the management hierarchy. Administrators don't have to be on the sales team or members of territories.
- Deal Protection: Salespeople assigned to an opportunity retain the sales credit on an opportunity even if they're moved to another opportunity.

# How Sales Users Gain Access to Oracle Sales in the Redwood User Experience Objects

Three objects are specific to Oracle Sales in the Redwood User Experience (Sales in the Redwood UX): the Sales Contests object, the Sales Goals object, and the Sales KPI object. Sales users with access to the Sales in the Redwood UX UIs gain access to these object records through several access paths.

## How Users Gain Access to Sales Contests

You can access data about a sales contest if you're the owner of the contest, are a participant in the contest, or if you're in the management hierarchy of the owner or a participant. All users who have access to a contest can view data for all contest participants. Specifically, you can access a sales contest if:

- You create the contest. If you create a contest, you're the contest owner.

  Sales Managers, Sales VPs, and the Sales Administrators can create contests. Sales Managers and Sales VPs can only add participants from their own downward hierarchy to the contest. Sales Administrators can add any users as participants.
- You're a participant in the contest.

  Users added to a contest can view contest data for themselves and for all other participants in the contest.
- The contest owner or participant is your direct or indirect report in the resource hierarchy.

  You can view contest details for your reports.
- The user who owns the contest can edit or delete the contest.
- Sales administrators can view all contests and can edit and delete any contest.

Once a contest is running, the contest owner, all participants, and the management hierarchy of the participants receive access to view the contest. Everyone who gets access to the contest can see the same information. So, for example, contest participants can see each other's scores on a given KPI, along with statistics such as the daily average score of each participant.

# How Users Gain Access to Sales Goals

Whether or not you can access data about a particular sales goal depends on your membership in the resource hierarchy and whether or not you're a goal participant. In general, you can access goal data for yourself and for your direct and indirect reports. Specifically, you can access a goal if:

- You create the goal.

  The user who creates the goal can view the goal and can edit and delete the goal.

  Sales Managers, Sales VPs, and the Sales Administrator can create goals. When creating a goal, Sales Managers and Sales VPs can only add users from their own downward resource hierarchy as participants of the goal. Sales Administrators can add any users as goal participants.
- You're a participant of the goal.

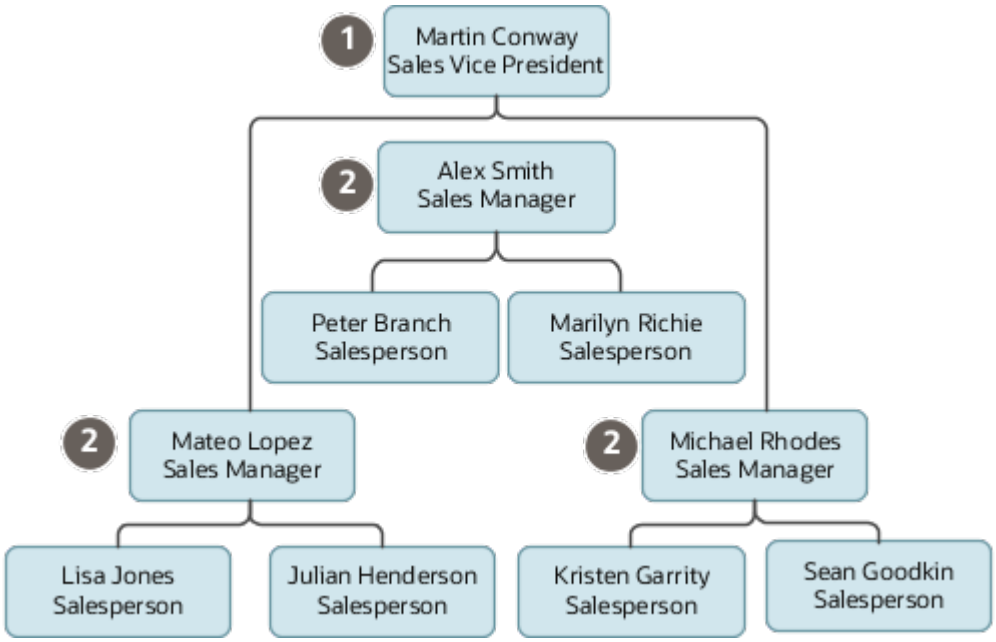
  Each participant can see only their own goal target and progress.
- The goal owner or participant is your direct or indirect report in the resource hierarchy.

  Members of the management hierarchy of a goal participant can view goal data and edit targets for goal participants in their own downward resource hierarchy.

  For example, the following figure shows an example sales hierarchy consisting of a sales VP who has three sales managers reporting to him. Each of the sales managers has a team consisting of two direct reports. If Martin

Conway, the sales VP, sets a goal for all the sales people in his organization, then each member of the hierarchy has access to goal performance data according to their own position in the hierarchy as follows:

a. (Callout 1) Martin Conway can see goal performance data for each of the three sales teams and for each participant in each team.
b. (Callout 2) Each sales manager can see goal performance data for their direct reports. So Alex Smith can see goal data for Peter and Marilyn but not for any of the salespeople on Michael or Mateo's teams.
c. Each individual salesperson can see their own goal performance data but can't see goal data for anyone else.




- Sales administrators can access all goals and all goal participants, and can edit and delete any goal.

## How Users Gain Access to Sales KPIs

Oracle provides a number of predefined key performance indicators (KPIs) that sales managers can use for creating goals and contests but you can also create your own KPIs. All users can view KPIs but only sales administrators can create and manage KPIs. You can access sales KPI data as follows:

- All users can view the predefined sales KPIs.

  Sales Managers, Sales Representatives, Sales VPs, and Sales Administrators can view the predefined sales KPIs.
- Only sales administrators can create custom KPIs.

  Sales Managers, Sales Representatives, and Sales VPs can view all active, custom sales KPIs.
- Sales administrators can update, delete, and change the status of custom KPIs. Sales administrators can also change the status of predefined KPIs and can copy predefined KPIs.

# Multiple Business Units and Data Access for Sales Objects

The way that you implement multiple business unit functionality in your enterprise can affect your users' access to object transactional data.

A business unit (BU) is a part of an enterprise that performs one or more business functions, such as sales or marketing. BUs let you both separate and share setup data. BUs also can control transactional data access. When you first implement the applications, your enterprise structure has a single BU, and all of your users belong to that one BU. You can create more BUs if you need to.

Resource organizations are mapped to one or more BUs, and users get associated with BUs through their resource organization membership. When you create a sales user and assign the user to a resource organization, the user gains access to each BU that's mapped to the resource organization. For example, users can access relevant transactional data associated with their primary BU, but might also have access to relevant transactional data in other BUs through their resource organization.

> **Note:** When you create a user in the sales application, you specify a BU for the user. But only the BUs associated with the user's resource organization are relevant in determining the BUs a user can access. If a BU isn't specified for a resource organization, the default BU is used.

Within Sales, these business objects support the use of multiple BUs:

- Contracts
- Leads
- Opportunities
- Resource Organizations
- Territories

When you create an object that supports multiple BUs, such as an opportunity, you specify the BU to associate with the object.

## Object Access in a Single BU Environment (Default)

In this type of implementation, all users can access master data, such as product or account information, by default. Users also have access to transactional data for objects such as opportunities, contracts or leads:

- Sales administrators can access transactional data for all objects.

- Sales users gain access to transactional data for an object through one of these methods:
  - They have been granted full access to the object
  - Through territory or team membership
  - Through the resource management hierarchy

Full access to an object is provided through data security policies that include a condition of All Values. This table provides information about other methods of object access:

***More Ways to Gain Access to Objects***

| Type of Object Access | Description |
|---|---|
| Territory membership | You gain access to an object if:<br>- You're the owner or member of the territory that's assigned to the object.<br>- You're the owner or member of an ancestor territory of the territory assigned to the object.<br>- Your direct or indirect report in the resource hierarchy is the owner or a member of the territory assigned to the object.<br>- Your direct or indirect report in the resource hierarchy is the owner or member of an ancestor territory of the territory assigned to the object. |
| Team membership | You gain access to an object if:<br>- You're a member of the sales team assigned to the object.<br>- Your direct or indirect report in the resource hierarchy is a member of the sales team assigned to the object .<br>- You're a member of the partner team assigned to the object. |

## Object Access in a Multiple BU Environment

In a multiple BU environment, access to objects and data is influenced by the BU the user belongs to. In this type of implementation, access to transactional data for objects, such as opportunities or leads, is determined in these ways:

- Sales administrators can access transactional data for all objects that are associated with the BU or units to which the administrators are assigned.
- Sales users access to transactional data for an object is the same in multiple BU environments and single BU environments. So sales users can access object data across BU boundaries provided that they have valid access to the object by means of territory or team membership, through the resource hierarchy, or by being granted full access to the object.

  But BU assignment can indirectly affect a user's access to object transactional data. In a multiple BU environment, BUs are available as territory dimensions and can be included as part of the territory coverage definition for the assignment of transactions. A sales user gains access to object data through territory membership. If BU is specified as a territory dimension, then the user's access to data is limited to objects which, when they were created, were assigned to the same BU that's assigned to the user's territory team.

For additional information about using multiple BUs, see the Oracle Fusion Cloud Sales Automation: Implementation Reference guide.

*Related Topics*

- Overview of Sales Resources and Multiple Business Units
- Associate Resource Organizations with Multiple Business Units

# Configure Data Access in a Multiple Business Unit Environment

You can configure the default data security settings for your sales users by creating a custom version of the role users are assigned. Depending on whether you're using access groups or data security policies, you can then edit the custom role, or system access group generated for the custom role, to provide the access to object data you need.

The conditions specified in access group rules or data security policies can use several components as mechanisms for sharing data. So one important consideration to keep in mind when configuring users' access to data is that users might have access to object records through more than one access path. For example, a user assigned a role that grants access to opportunities based on team and territory can access the opportunity through both access paths independently. To limit this access, you have to remove or modify the access group rules or data security policies that provide access using either path.

For example, in a multiple business unit (BU) environment, users from different BUs might be assigned to an account team. In this scenario, you might want salesperson on the account team to be able to view only opportunities they created, but not opportunities created by their team members.

Here's how to restrict users' access to opportunities using access groups and rules:

1. Sign in to the sales application as a user who has the IT Security Manager job role.
2. Create a copy of the Sales Representative job role in the Security Console, for example Sales Representative Custom, and assign the role to at least one user.

   A custom access group, Sales Representative Custom Group, is created for the custom role but isn't associated with any predefined access group rules.

   > **Note:** System access groups are generated only for job roles that have at least one user associated with them.

3. Navigate to the Sales and Service Access Management work area **Navigator** > **Tools** > **Sales and Service Access Management**.

   The Access Groups page is displayed listing any existing active access groups.
4. Search for and select the Sales Representative Custom Group generated for the custom role you created in step 2.
5. On the Edit Access Group: Overview page, click the Object Rules tab, then select **Opportunity** from the **Object** drop-down list.
6. Click **Add Rule**.
7. Select the **Opportunity Owner** rule, click **Apply**, then click **Done**.

   This rule provides group members with access to opportunities they own. As you don't want group members to have access to opportunities through access paths other than opportunity ownership, such as through account team membership or territory membership, there's no need to assign any other rules to the group.
8. Click **Save and Close**.

9. On the Edit Access Group: Object Sharing Rules page, in the **Access Level** field select the access level for the rule you've just added, then make sure the **Enable** checkbox is selected to enable the rule.
10. Click **Save and Close** to save the changes you made to the access group.
11. Provision the Sales Representative Custom job role instead of the Sales Representative job role to relevant users.

    Users provisioned with the Sales Representative Custom job role are automatically added as members of the Sales Representative Custom Group access group and receive access to only those opportunities they own.

Here's how to restrict users access to opportunities using data security policies:

1. Create a copy of the Sales Representative job role in the Security Console, for example Sales Representative Custom.
2. Edit the new Sales Representative Custom role.
3. Navigate to the Edit Role: Data Security Policies page of the Security Console.
4. Remove any policies defined for the opportunity object that contain conditions that provide opportunity access through access paths other than opportunity ownership, such as through account team membership or territory membership.

    - Team membership. To remove users access to opportunities created by their account team members or members of the territory associated with the account, remove all policies with this condition:

      ```
      Access the opportunity for table MOO_OPTY where you are member or in management chain of
      opportunity account team, account territory team or upward territory hierarchy
      ```

    - Territory membership. Remove users access to opportunities they can access through opportunity territory membership.

      Users might have access to opportunities through their membership of the territory associated with the opportunity. For example, user A might be an account team member and also a member of a territory (for example, the NW territory) that isn't assigned to the account. If a second user B, who is not an account team member, creates an opportunity for the account, and the opportunity is assigned to the NW territory, user A gains access to the opportunity record through territory membership. To remove this access, remove all policies that contain this condition:

      ```
      Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity
       territory team or a territory resource with a descendant territory in the opportunity territory
       team
      ```

5. Save the custom role you created and provision this role to users instead of the Sales Representative job role.

    Users assigned this role only have access to opportunities on the account that they created themselves.

For additional information about access groups, see the Access Groups chapter. For additional information about configuring data security, see the chapter Configure and Troubleshoot Data Security.

*Related Topics*

- Overview of Data Security Configuration
- Copy Job or Abstract Roles
- Overview of Access Groups

# Data Sharing and Visibility in Incentive Compensation

The conditions specified in data security policies control visibility to record-level data associated with a schema object, such as an incentive compensation plan and a paysheet.

Conditions can use these components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

- Business unit
- Analyst assignment
- Person security profile

## Business Unit

For incentive compensation administrators, the basis for data sharing is the business unit they have access to. Incentive compensation administrators are users assigned to these job roles:

- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst

## Analyst Assignment

You have the option to further limit data access for users assigned to the Incentive Compensation Analyst role. You can limit the analyst access to the business unit or to participants who are directly assigned to the analyst. In the Setup and Maintenance work area, use the following:

- Offering: Sales
- Functional Area: Incentives
- Task: Manage Parameters

For example, analyst Amy is directly assigned to the participants Jack and Ravi. Analyst Ryan is assigned to the participants Juan and Mary. When the Manage Parameter setting indicates analyst security is by participant, Amy can't manage participant data for Juan and Mary because she isn't the assigned analyst. This functionality applies to data within the Participant Snapshot and Payments work areas.

You can assign analysts to participants when the participants are imported, using the Participant Assignments, Manage Analyst Assignments task, and using the Participant Snapshot, Participant Details task.

## Person Security Profile

The predefined person security profile types can be assigned to abstract roles, such as the employee, line manager, and contingent worker roles. You can also assign the security profile to the Incentive Compensation Participant and Incentive Compensation Participant Manager abstract roles. The person security profile, view own record option provides visibility to the participant's own data. The person security profile, view manager hierarchy option provides the participant manager with visibility to participant data for the subordinates in their management hierarchy.

# Data Sharing and Visibility in Service

A service application user's access to service requests is determined by the set of access group rules or data security policies associated with all the roles the user is provisioned with.

The predefined roles in the service application don't provide for service request visibility based on business unit or queue. But you can configure either queue or BU-based visibility to service requests for specific roles. Users assigned these roles can see only the service requests assigned to the business unit or queue where they're a resource member.

For more information about restricting service request visibility by business unit or by queue, see the Fusion Service: Implementing Service Center with the Classic User Experience guide.

*Related Topics*

- How do I set up request visibility based on queue?
- How You Set Up Visibility Based on BU

# 3 Initial Security Setup Tasks

## Overview of Applications Security Setup Tasks

If you're assigned the IT Security Manager job role, then during implementation you can prepare the application security environment. These are some of the security setup tasks:

- Manage Applications Security Preferences

  This task opens the Administration tab of the Security Console. Select the appropriate tab of the Security Console to set enterprise-wide preferences that affect users, roles, and notifications to application users.
- Import Users and Roles into Application Security

  This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables.
- Import User Login History

  This task runs a process that imports the history of user access to Oracle Fusion Applications. This information is required by the Inactive Users Report.
- Run User and Roles Synchronization Process

  This task runs a process that copies data from the LDAP directory to Oracle Fusion Applications Security tables.
- Verify your data security setup

  If you were provisioned with the sales and service application for the first time in release 22B or later, verify your data security setup in the Sales and Service Access Management work area.

Many of the security setup tasks can be run from the Users and Security functional area of the Sales offering in the Setup and Maintenance work area.

*Related Topics*

- Application Security Preferences
- Import Users and Roles into Applications Security
- Synchronize User and Role Information
- Verify Your Data Security Setup

## Oracle Cloud Applications Security Console

Use the Security Console work area to perform most security-management tasks.

See also: *Configure the Security Console*

## Security Console Tasks

You can do these tasks on the Security Console:

- Review role hierarchies and role analytics.
- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.

  > **Note:** You use the Manage Users work area, not the Security Console, to create users and to provision users with roles.

- Compare roles.
- Simulate the Navigator for a user or role.
- Manage the default format of user names and the enterprise password policy.
- Manage notifications for user-lifecycle events, such as password expiration.
- Manage PGP and X.509 certificates for data encryption and decryption.

  > **Note:** Oracle Sales and Fusion Service don't use certificate functionality.

- Set up federation and sync user and role information between Oracle Applications Security and Microsoft Active Directory, if appropriate.

## Security Console Access

You must have the IT Security Manager job role to use the Security Console. You open the Security Console by clicking the **Security Console** link within the **Tools** menu in the Navigator. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Manage Job Roles
- Manage Duties
- Manage Data Security Policies

You might also be interested in reviewing the article, *How to Audit Security Customization (Role Creation, Role Modification, Role Membership, Entitlement/ Privilege Changes) in Fusion Application (Doc ID 2175861.1)*, on My Oracle Support.

# Import Users and Roles into Applications Security

Before you can use the Security Console to implement security, you must initialize the Oracle Fusion Applications Security tables with existing user and role information. To do this, perform the Import Users and Roles into Application Security task.

## Run the Import User and Role Application Security Data Process

Sign in as a setup user and follow these steps:

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

- Offering: Sales
- Functional Area: Users and Security
- Task: Import Users and Roles into Application Security

2. On the Import Users and Roles into Application Security page, click **Submit**.

This action starts the Import User and Role Application Security Data process. Once the process completes, you can use the Security Console.

**Note:** Oracle recommends that you schedule this process to run daily.

*Related Topics*

- Schedule the Import User and Role Application Security Data Process
- How do I update existing setup data?

# Synchronize User and Role Information

Run the Retrieve Latest LDAP Changes process once during implementation to initialize the Oracle Fusion Applications tables.

User accounts for Oracle Fusion Applications users are maintained in your Lightweight Directory Access Protocol (LDAP) directory. The LDAP directory also stores information about the roles provisioned to users. During implementation, any existing information about users and their roles must be copied from the LDAP directory to the Oracle Fusion Applications tables. After that, the data is synchronized automatically. To copy this user and role information, use the task Run User and Roles Synchronization Process. This task calls the Retrieve Latest LDAP Changes process.

## Run the Retrieve Latest LDAP Changes Process

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Run User and Roles Synchronization Process
2. On the process submission page for the Retrieve Latest LDAP Changes process, click **Submit**.
3. Click **OK** to close the confirmation message.

*Related Topics*

- How do I update existing setup data?

# Application Security Preferences

There are a number of options on the Security Console that you can use to control the default behavior of functionality such as working with roles or certificates.

Some of these options can be overridden, but it's a good idea to set these options during implementation, before you start to create application users or configure your security environment.

To configure the security preferences, the initial user, or a setup user with the IT Security Manager job role, performs the task Manage Applications Security Preferences. This task opens the Administration tab of the Security Console from where you can set these default values and preferences:

- On the General subtab of the Security Console Administration tab, you can set these values:
  - Specify for how long certificates remain valid by default.

    **Note:** The sales and service applications don't use certificate functionality.
  - Specify how often a warning appears to remind Security Console users to import latest user and role information.
- On the Roles subtab of the Security Console Administration tab, you can set these values:
  - Specify default prefix and suffix values for copied roles.
  - Specify a limit to the number of nodes that can appear in graphical representations of roles on the Roles tab of the Security Console.
  - Specify whether hierarchies on the Roles tab appear in graphical or tabular format by default.
- On the User Categories tab of the Security Console, you can set these values:
  - Create user categories and add users to a category.
  - Specify the default format of user names for the user category.
  - Manage the password policy for a user category.
  - Manage the notification of user and password events to users in a selected user category.
  - Create notification templates for a user category.

You can also configure security preferences by navigating directly to the Security Console (**Navigator** > **Tools** > **Security Console**). For detailed information about configuring default functionality for user names, roles and notifications, see the topics in the remainder of this chapter. For information about configuring the password policy for a user category, see the chapter Manage Passwords.

Options on the Security Console also allow you to implement location-based access, to configure a bridge between Oracle Applications Cloud and Microsoft Active Directory, and to set up single sign-on authentication. For information on these configuration tasks, see the relevant chapters in the guide.

# Set the Default User Name Format

During implementation, you specify the default format of user names for users in the default user category. The default format is used to automatically generate a user name for a user if you don't specify one when creating the user.

This topic describes how to specify the default format of user names and the formats that are available.

## Specify the Format of User Names

1. In the Setup and Maintenance work area, go to:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Applications Security Preferences

    The Administration page of the Security Console opens.

    > **Tip:** You can navigate directly to the Security Console at any time by clicking **Security Console** from the Navigator.

2. Click the **User Categories** tab, then click the name of the default user category to open it.
3. Click **Edit** on the Details subtab.
4. In the **User Name Generation Rule** field, select one of the available user name formats.

    This table describes the available user name formats.

| Format Name | Description |
|---|---|
| Email | The work email (or party email, for party users) is the user name. For example, the user name for john.smith@example.com is john.smith@example.com. To make duplicate names unique, a number is added. For example, john.smith2@example.com may be used if john.smith@example.com and john.smith1@example.com already exist.<br><br>**Email** is the default format. |
| FirstName.LastName | The user name is the user's first and last names separated by a single period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user's middle name or a random character is used. For example, John Smith's user name could be john.frank.smith or john.x.smith. |
| **FLastName** | The user name is the user's last name prefixed with the initial of the user's first name. For example, the user name for John Smith is jsmith. |
| Person or party number | The person or party number generated by the application is the user name. For example, if John Smith's party number is 100000000178803, then the user name is 100000000178803. |

| Format Name | Description |
|---|---|
| | Because user names generated from party or person numbers can be difficult to remember you might prefer not to select this option. |

5. Enable or disable the option **Generate system user name when generation rule fails**. This option controls whether a system user name is generated if the user name rule fails. For example, a user name rule will fail if the default user name format is party number or email but these values aren't available when the user is created.
    - If the option is enabled, a system user name is generated by applying these options in the following order until a unique user name is defined:
        i. Email
        ii. FirstName.LastName
        iii. If only the last name is available, then a random character is prefixed to the last name.
    - If the option is disabled, then an error is raised if the user name can't be generated in the selected format.
6. Click **Save and Close**. Any changes take effect immediately.

## Edit User Names

When creating users on the Create User page, you can enter user names in any format to override the default user names. You can also edit user names for individual users on the Edit User page.

*Related Topics*

- How do I update existing setup data?

# Role Preferences

Select default role preferences for the enterprise during implementation. To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. From there, click the Roles subtab to display the Role Preferences page.

## Copied-Role Names

It's best practice when creating roles to copy predefined roles and edit the copied versions of the roles. When you copy a predefined role:

- The **ORA_** prefix, which identifies predefined roles, is removed automatically from the role code of the copied role.
- The enterprise prefix and suffix values are added automatically to the role name and code of the copied role.

You specify enterprise prefix and suffix values on the Role Preferences page. These are the default values:

- Prefix values are blank.

- The role-name suffix is **Custom**.
- The role-code suffix is **_CUSTOM**.

For example, if you copy the Channel Account Manager job role (ORA_ZPM_CHANNEL_ACCOUNT_MANAGER_JOB), then the default name and code of the copied role are:

- Channel Account Manager Custom
- ZPM_CHANNEL_ACCOUNT_MANAGER_JOB_CUSTOM

You can supply prefix values and change the suffix values on the Role Preferences page as required. If you change these values, click **Save** and the changes take effect immediately.

## Graph Nodes and Default Views

On the Roles tab of the Security Console, you can display role hierarchies. By default, these hierarchies appear in tabular format. If you want to display role hierarchies in graphical format by default instead, deselect the **Enable default table view** option on the Role Preferences page.

When role hierarchies appear on the Roles tab, the number of nodes can be very high. You can limit the number of nodes by setting the **Graph Node Limit** option on the Role Preferences page. When you display a role hierarchy with more nodes than the specified limit, gray arrows indicate additional nodes. You can set such a node as the focus node to see the rest of its hierarchy.

# Overview of User Categories

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

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

- Users have different preferences in receiving automated notifications from the Security Console. For example, employees of your organization using the organization's single sign-on don't require notifications from the Security Console about creating new users, password expiry, or password reset. However, the suppliers of your organization who aren't using the organization's single sign-on, must receive such notifications from the Security Console.
- You have built an external application for a group of users using the REST APIs of Oracle Fusion Applications. You intend to redirect this user group to the external application when using the Security Console to reset passwords or create new users.

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

- Segregate users into categories
- Specify Next URL
- Set user preferences
- Define password policy
- Enable notifications

## Segregate Users into Categories

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

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

## Specify Next URL

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

## Set User Preferences

Select the default format of the User Name, the value that identifies a user when signed in. It is generated automatically in the format you select. For additional information, see the topic Set the Default User Name Format.

## Define the Password Policy

Determine the password policy for a user category. For example, specify the number of days a password remains valid or select a password format. For additional information, see the topic Password Policy.

## Enable and Disable Notifications

You can enable and disable the email notifications sent to users when specific events occur. For additional information, see the topic Enable Notifications.

*Related Topics*

- Set the Default User Name Format
- Enable Notifications
- Password Policy
- REST API for Common Features in Oracle Applications Cloud

# Add Users to a User Category

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

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

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

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

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

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

## Adding Users to a New User Category

To create a user category and add users:

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

## Adding Users to an Existing User Category

To add users to an existing user category:

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

## Specifying the User Category for an Existing User

To add an existing user to a user category:

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

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

# Enable Notifications

Notifications are enabled by default, but you can disable them if required.

You can also enable or disable notifications separately for each user category. If users belonging to a specific category don't want to receive any notification, you can disable notifications for all life-cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.

Notifications are sent for a set of predefined events. To trigger a notification, you must create a notification template and map it to the required event. Depending on the requirement, you can add or delete a template that's mapped to a particular event.

> **Note:** You can't edit or delete predefined notification templates that begin with the prefix ORA. You can only enable or disable them. However, you can update or delete the user-defined templates.

User Category feature supports both SCIM protocol and HCM Data Loader for performing any bulk updates.

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

*Related Topics*

- Create Notification Templates
- How can I enable or disable notifications for users?

# User Name and Password Notifications

Users in all user categories get notified automatically of changes to their user accounts and passwords by default. These notifications are based on notification templates.

During setup, plan which notifications to use for each user category and disable any that aren't needed. Many templates are predefined, but you can also create templates for a user category.

## Predefined Notification Templates

This table describes the predefined notification templates. Each template is associated with a predefined event. For example, the Password Reset Template is associated with the password reset event. You can see these notification templates and their associated events on the User Category: Notifications page of the Security Console for a user category.

***Predefined Notification Templates***

| Notification Template | Description |
|---|---|
| Password Expiry Warning Template | Warns the user that a password is expiring soon and provides instructions for resetting the password. |

| Notification Template | Description |
|---|---|
| Password Expiration Template | Notifies the user that a password has expired and provides instructions for resetting the password. |
| Forgot User Name Template | Sends the user name to a user who requested the reminder. |
| Password Generated Template | Notifies the user that a password has been generated automatically or manually changed, and provides instructions for resetting the password. |
| Password Reset Template | Sends a reset-password link to a user who requested a new password.<br>Users can request new passwords by selecting the **Forgot Password** link on the application Sign In page, or by selecting the **Password** option on the Preferences page. To navigate to the Preferences page, click your user image or name in the global header to open the **Settings and Actions** menu, then select the **Set Preferences** option. |
| Password Reset Confirmation Template | Notifies the user when a password has been reset. |
| New Account Template | Notifies a user when a user account is created and provides a reset-password link. |
| New Account Manager Template | Notifies the user's manager when a user account is created. |

When you create a user category, it's associated automatically with the predefined notification templates, which are all enabled.

You can't edit the predefined templates but you can create templates and disable the predefined versions. Each predefined event can be associated with only one enabled notification template at a time.

> **Note:** If you're using the sales application with Oracle Fusion Cloud Human Resources, more notification templates are available that you can use to redirect user name and password notifications to a user's manager, if the user doesn't have a work email. For more information, see the *Securing HCM* guide.

# Create a Notification Template

Predefined notification templates exist for events related to the user-account life cycle, such as user-account creation and password reset. When templates are enabled, users are notified automatically of events that affect them. To provide your own notifications, you create notification templates.

Follow these steps to create a notification template:

1. Open the Security Console and click the User Categories tab.
2. On the User Categories page, click the name of the relevant user category.
3. On the User Categories: Details page, click the Notifications subtab.
4. On the User Category: Notifications page, click **Edit**.
5. Click **Add Template**.
6. In the Add Notification Template dialog box:
    a. Enter the template name.
    b. In the **Event** field, select a value. The predefined content for the selected event appears automatically in the **Message Subject** and **Message Text** fields. Tokens in the message text are replaced automatically in generated notifications with values specific to the user.
    c. Update the **Message Subject** field, as required. The text that you enter here appears in the subject line of the notification email.

d. Update the message text, as required.

This table shows the tokens supported in the message text.

| Token | Meaning | Events |
|---|---|---|
| userLoginId | User name | - Forgot user name<br>- Password expired<br>- Password reset confirmation<br>- New account created |
| firstName | User's first name | All events |
| lastName | User's last name | All events |
| managerFirstName | Manager's first name | - New account created - manager<br>- Password reset confirmation - manager<br>- Password reset - manager |
| managerLastName | Manager's last name | - New account created - manager<br>- Password reset confirmation - manager<br>- Password reset - manager |
| loginURL | URL where the user can sign in | - Expiring external IDP signing certificate<br>- Password expired<br>- Password expiry warning |
| resetURL | URL where the users can reset their password | - New account created - manager<br>- New user created<br>- Password generated<br>- Password reset<br>- Password reset - manager |
| CRLFX | New line | All events |
| SP4 | Four spaces | All events |
| adminActivityUrl | URL where an administrator initiates an administration activity | Administration activity requested |
| providerName | External identity provider | Expiring external IDP signing certificate |
| signingCertDN | Signing certificate | Expiring external IDP signing certificate |

| Token | Meaning | Events |
|---|---|---|
| signingCertExpiration | Signing certificate expiration date | - Expiring external IDP signing certificate<br>- Expiring service provider signing certificate |
| encryptionCertExpiration | Encryption certificate expiration date | Expiring service provider encryption certificate |
| adminFirstName | Administrator's first name | - Administration activity location-based access disabled confirmation<br>- Administration activity single sign-on disabled confirmation |
| adminLastName | Administrator's last name | - Administration activity location-based access disabled confirmation<br>- Administration activity single sign-on disabled confirmation |

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

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

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

# Notifications for Users Based on Status

Security Console sends notifications to users for important events that occur in the application. However, some notifications aren't sent to users if they're inactive or have been locked out of the application.

Here's the list of notifications that are either sent or not sent to users based on their status:

| Template Name | Event Name | When is the notification sent? | Sent to Inactive Users? | Sent to Locked Users? |
|---|---|---|---|---|
| ORA Expiring External IDP Signing Certificate | Expiring External IDP Signing Certificate | When an external identity provider certificate is about to expire | No | Yes |
| ORA Expiring Service Provider Encryption Certificate | Expiring service provider encryption certificate | When a service provider encryption certificate is about to expire | No | Yes |
| ORA Expiring Service Provider Signing Certificate | Expiring service provider signing certificate | When a service provider signing certificate is about to expire | No | Yes |

| Template Name | Event Name | When is the notification sent? | Sent to Inactive Users? | Sent to Locked Users? |
|---|---|---|---|---|
| ORA Forgot User Name | Forgot user name | When a forgot user name request is processed | No | Yes |
| ORA Password Expiration | Password expired | When a password has expired | No | No |
| ORA Password Expiry Warning | Password expiry warning | When a password expiry warning is sent | No | No |
| ORA Password Reset Confirmation Manager | Password reset confirmation - manager | When a password is changed and the manager must be notified | No | Yes |
| ORA Password Reset Confirmation | Password reset confirmation | When a password is changed | No | Yes |
| ORA Password Reset Manager | Password reset - manager | When a password is reset and the manager must be notified | No | Yes |
| ORA Password Reset | Password reset | When a password reset request is processed | No | Yes |
| ORA Administration Activity Request Template | Administration activity request | When an administrator initiates an administration activity | Yes | Yes |
| ORA Location Based Access Disabled Confirmation | Administration activity location-based access disabled confirmation | When an administrator disables location-based access through an administration activity request | Yes | Yes |
| ORA New Account Manager | New account created - manager | When a new account request is processed and the manager must be notified | Yes | Yes |
| ORA New Account | New user created | When a new account request is processed | Yes | Yes |
| ORA Password Generated | Password generated | When a password is issued | Yes | Yes |
| ORA Single Sign-On Disabled Confirmation | Administration activity single sign-on disabled confirmation | When an administrator disables single sign-on through an administration activity request | Yes | Yes |

# Schedule the Import User Login History Process

During implementation, you perform the Import User Login History task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables.

This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform the **Import User Login History** task for the first time, you're recommended to schedule it to run daily. In this way, you can ensure that the Inactive Users Report is up to date.

## Schedule the Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User Login History** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times.
9. Click **Submit**.
10. Click **OK** to close the **Confirmation** message.

*Related Topics*

- Inactive Users Report

# Why You Run the Send Pending LDAP Requests Process

It's best practice to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to your LDAP directory server. Schedule the process in the Scheduled Processes work area. This topic describes the purpose of Send Pending LDAP Requests.

Send Pending LDAP Requests sends the following items to the LDAP directory:

- Requests to create, suspend, and reactivate user accounts.
    - When you create a person record for a worker, a user-account request is generated automatically.
    - When a person has no roles and no current work relationships, a request to suspend the user account is generated automatically.
    - A request to reactivate a suspended user account is generated automatically if you rehire a terminated worker.

  The process sends these requests to the LDAP directory unless the automatic creation and management of user accounts are disabled for the enterprise.

- Work e-mails.
  If you include work e-mails when you create person records, then the process sends those e-mails to the LDAP directory.
- Role provisioning and deprovisioning requests.
  The process sends these requests to the LDAP directory unless automatic role provisioning is disabled for the enterprise.
- Changes to person attributes for individual users.
  The process sends this information to the LDAP directory unless the automatic management of user accounts is disabled for the enterprise.

All of these items are sent to the LDAP directory automatically unless they're either future-dated or generated by bulk data upload. You run the process Send Pending LDAP Requests to send future-dated and bulk requests to the LDAP directory.

> **Note:** Only one instance of Send Pending LDAP Requests can run at a time.

*Related Topics*

- Avoid Having Too Many Processes Run at the Same Time

# Schedule the Send Pending LDAP Requests Process

The Send Pending LDAP Requests process sends bulk requests and future-dated requests that are now active to your LDAP directory. You're recommended to schedule the Send Pending LDAP Requests process to run daily. This procedure explains how to schedule the process.

> **Note:** Schedule the process only when your implementation is complete. After you schedule the process you can't run it on an as-needed basis, which may be necessary during implementation.

## Schedule the Send Pending LDAP Requests Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
3. In the Schedule New Process dialog box, search for and select the **Send Pending LDAP Requests** process.
4. In the Process Details dialog box, set **User Type** to identify the types of users to be processed. Values are **Person**, **Party**, and **All**. You're recommended to leave **User Type** set to **All**.
5. The **Batch Size** field specifies the number of requests in a single batch. For example, if 400 requests exist and you set **Batch Size** to **25**, then the process creates 16 batches of requests to process in parallel.
   The value **A**, which means that the batch size is calculated automatically, is recommended.
6. Click **Advanced**.
7. On the Schedule tab, set **Run** to **Using a schedule**.
8. In the **Frequency** field, select **Daily**.
9. Enter the start and end dates and times.

10. Click **Submit**.

**Note:** Only one instance of Send Pending LDAP Requests can run at a time.

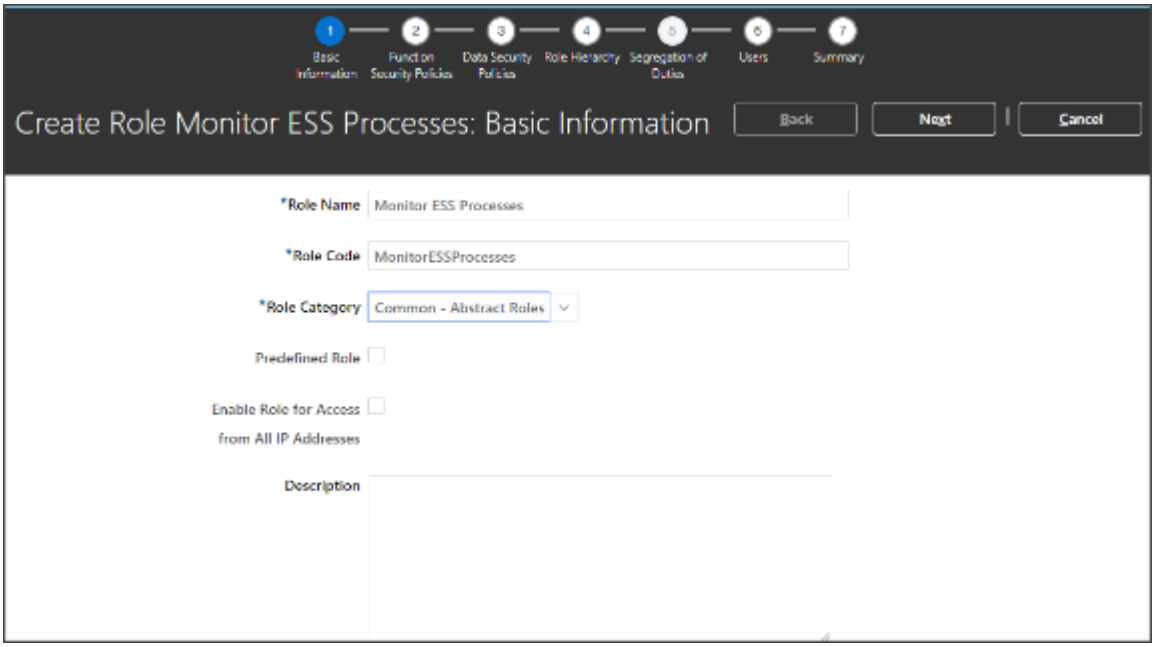
*Related Topics*

- Why You Run the Send Pending LDAP Requests Process
- Avoid Having Too Many Processes Run at the Same Time

# Give Users the Permission to View All Scheduled Processes

Your application setup requires you to run numerous scheduled processes and ensure they complete successfully. By default, users can only see the scheduled processes they themselves submit. By creating a custom role in the Security Console and assigning all of the setup users to it, you ensure that everyone can see what processes are running and their status, no matter who submitted them. This setup applies to both CX Sales and Digital Sales.

1. Open the **Security Console**.
2. Click the **Roles** tab.
3. On the Roles tab, click **Create Role**.
   The Create Role page displays a series of steps you can click directly or reach using the **Next** button.

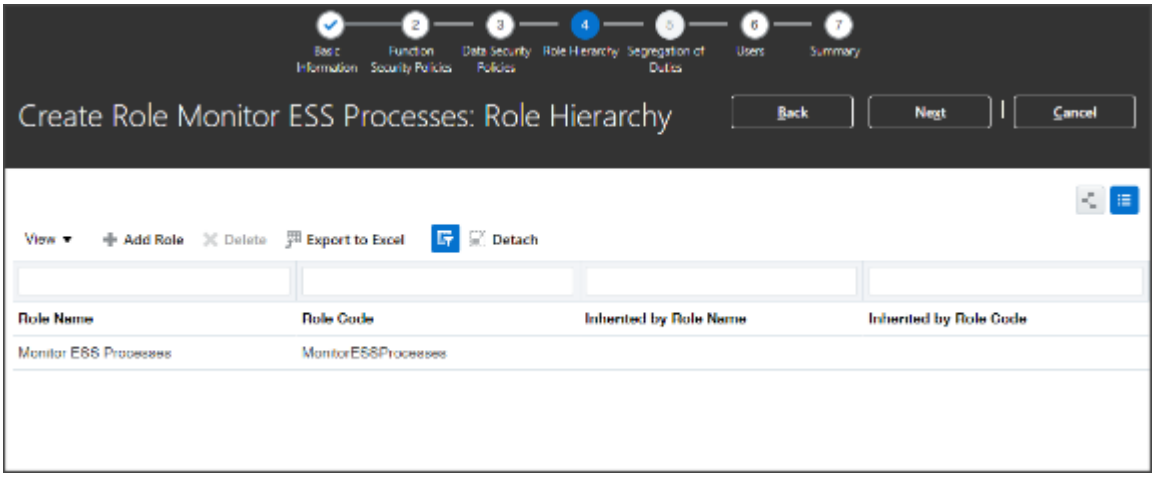



4. In the Create Role: Basic Information step, make the following entries:

| Field | Suggested Entry |
|---|---|
| Role Name | Monitor ESS Processes |

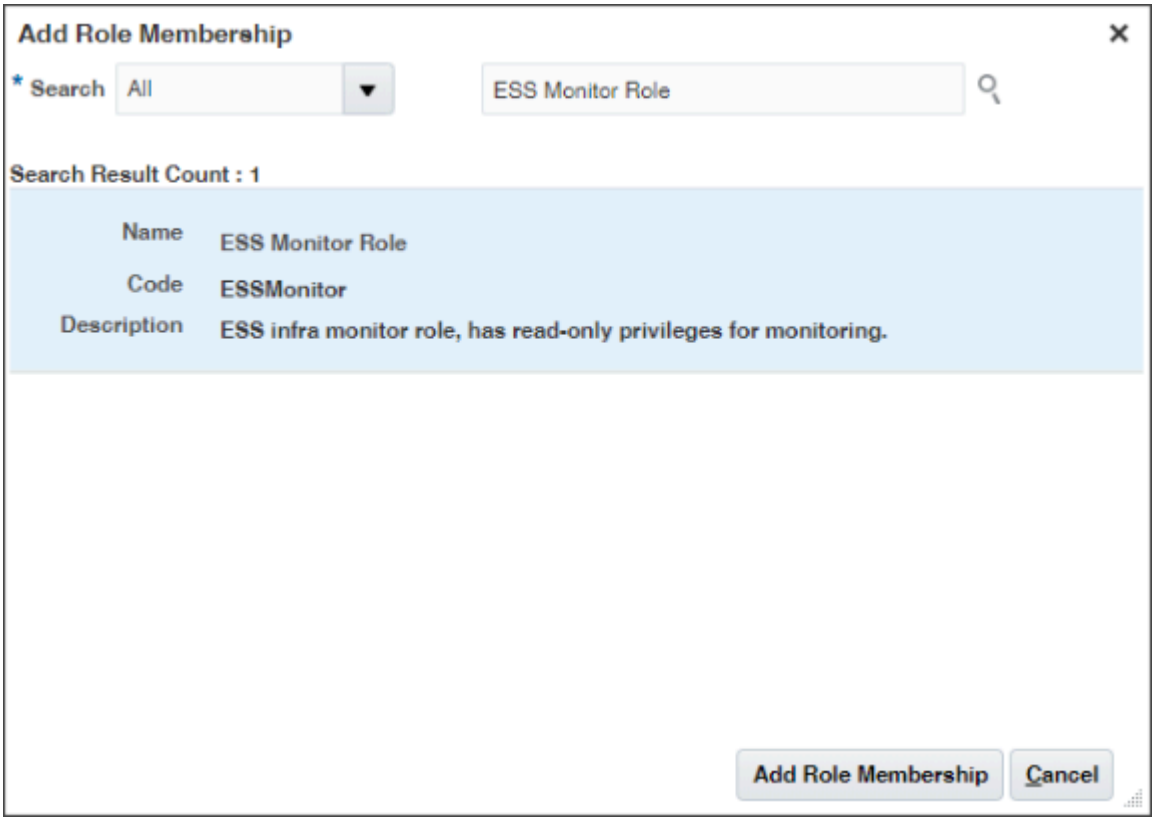
| Field | Suggested Entry |
|---|---|
| | |
| Role Code | MonitorESSProcesses |
| Role Category | Common -Abstract Roles |

5. Click the **Role Hierarchy** step.




6. Click **Add Role**.

7. In the Add Role Membership window, search for **ESS Monitor Role** and click **Add Role Membership**.




8. Click **Cancel** to close the Add Role Membership window.
9. Click the **Users** step.
10. Click **Add User** and add all of the setup users by searching for each by name and clicking **Add User to Role**.
11. Click **Cancel** when you are done.

    The Users step should list all of the users you added.
12. Click **Next** to get to the **Summary and Impact Report** step.
13. Click **Save and Close**.

    The users you added to the role can now monitor all of the scheduled processes in the **Schedule Processes** work area.

# Verify Your Data Security Setup

If you're using the sales and service application for the first time in release 22B or later, verify your data security setup before provisioning users with job roles.

Starting with release 22B, users receive access to sales data through access groups and their associated rules. When you assign job roles to users, they are automatically assigned membership of an associated system access group and receive all the data permissions provided by the access group object sharing rules.

When your environment was provisioned, a process was automatically run to publish and activate all the access group object sharing rules. To make sure that your new environment is ready to use, verify that the publish process completed successfully. If it didn't, you'll need to re-run the publish process. Here are the steps to use.

> **Note:** If you set up your security environment before release 22B, you don't have to perform the steps in this procedure. Your users receive data access through data security policies, or through a combination of data security policies and access group rules if you've configured one or more access groups or object sharing rules.

1. Sign in to the sales application as a user who has the IT Security Manager job role. The initial user provided by Oracle has this job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.

   The Configure Groups tab on the Sales and Service Access Management page is selected and displays the Access Groups page.
3. On the Access Groups page, click the Monitor tab.

   The Monitor page is displayed. From here, you can view all of the scheduled processes that are run to implement access group functionality.
4. Click the Publish Rules subtab and check the value of the **Status of Last Automatic Publish Process** field.
5. If the field has a value of **Succeeded**, there's nothing further to do.

   If the field has any other value, for example, **Error** or **Warning**, then run the publish process again using the steps in the topic Run the Publish Process to Setup Data Security.

*Related Topics*

- Overview of Access Groups

# Run the Publish Process to Setup Data Security

Publish and activate access group object sharing rules in your new sales application environment using the steps in this procedure.

> **Note:** You only need to perform the steps described in this topic if the automatically generated publish process that ran when your environment was provisioned didn't complete successfully.

1. Navigate to the Scheduled Processes work area (**Navigator** > **Tools** > **Scheduled Processes**).
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Perform Assignment Data Publish, Refresh, and Synchronization** process, then click **OK**.
4. In the Basic Options section of the Process Details dialog box, enter these values:
   - In the **Application** field, select **Object Sharing**.
   - In the **Owner Module** field, enter **PREDEFINED_RULE_PUBLISH**.
   - Select the **Publish** check box.
5. Click **Submit**.
6. On the Overview page, click the Refresh icon to verify that the publish job completed successfully.

   Once the process completes, you can view the log files for the process or get more details about the status by selecting your process in the Search Results table and reviewing the information in the Process Details or Status Details tabs.

# 4 Security and Personally Identifiable Information

## Overview

Securing and protecting confidential customer information against data breaches, data theft, or unauthorized access is an increasing concern for enterprises. To address this issue, Oracle restricts access to certain information, known as Personally Identifiable Information (PII), that's considered private to an individual.

Read this chapter to learn how personally identifiable information is secured in Oracle Applications Cloud.

For additional information about managing PII data, or about configuring access to PII data, see the guide Implementing Customer Data Management for CX Sales and Fusion Service at http://docs.oracle.com.

*Related Topics*

- Implementing Customer Data Management for Sales and Fusion Service

## How to Protect Personally Identifiable Information

The data or information that's used to uniquely identify a contact, or locate a person is called personally identifiable information (PII). Examples are social security number, addresses, bank account numbers, phone numbers, and so on.

This information is considered confidential and sensitive, and must be protected to prevent unautq horized use of personal information for the purposes of legal regulation, financial liability, and personal reputation. For example, only authorized users must be allowed access to the social security numbers of people stored in a system.

In Oracle Applications Cloud, the PII data is secured and can be accessed only by the following job roles with the exception of mobile phone data:

- Sales Administrator
- Enterprise Scheduler Job Application Identity for CRM
- Oracle Data Integrator Application Identity for CRM
- Web Services Application Identity for CRM

Mobile phone data is accessible to all seeded job roles. However, if access to mobile phone data is needed for custom job roles, the IT Security Manager must assign the required PII data policies to the custom job role in the Security Console. The IT Security Manager can also add data policies for other PII data to seeded job roles.

The following table lists the PII attributes that are secured in Oracle Applications Cloud.

**Note:** You can search privileges in Security Console using the Privilege Titles listed in the following table.

| PII Attribute | Table Name | Privilege Title |
|---|---|---|
| Taxpayer Identification Number (Social Security Number) | HZ_PERSON_PROFILES | View Trading Community Person Social Security |
| Taxpayer Identification Number (Social Security Number) | HZ_PERSON_PROFILES | Manage Trading Community Person Social Security |
| Citizenship Number | HZ_CITIZENSHIP | View Trading Community Person Citizenship Number |
| Citizenship Number | HZ_CITIZENSHIP | Manage Trading Community Person Citizenship Number |
| Home Address | HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITE_USES table | View Trading Community Person Address |
| Home Address | HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITE_USES table | Manage Trading Community Person Address |
| Home Phone | HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL | View Trading Community Person Contact |
| Home Phone | HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL | Manage Trading Community Person Contact |
| Mobile Phone | HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE | View Trading Community Person Mobile Phone Number |
| Mobile Phone | HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE | Manage Trading Community Person Mobile Phone Number |
| Home Email | HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL | View Trading Community Person Contact |
| Home Email | HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL | Manage Trading Community Person Contact |
| Additional Identifiers | All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS | View Trading Community Person Additional Identifier |
| Additional Identifiers | All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS | Manage Trading Community Person Additional Identifier |

# 5 Security and Reporting

## Security for Sales Analytics and Reports

Security for the analytics and reports that are delivered with the sales application is based on the roles that use each report. For example, sales managers can access sales analytics and reports that salespeople don't have access to.

Analytics are available throughout the sales application as embedded analytics and also in standalone mode by way of the transactional work areas. Sales users interact with information in Oracle Transactional Business Intelligence using Oracle Transactional Business Intelligence components, such as dashboards.

If you want to create new analytics or reports or edit existing ones, you should become familiar with sales security concepts and how access is secured to Oracle Transactional Business Intelligence subject areas, catalog folders, and reports.

### Subject Areas

Subject areas are functionally secured using duty roles. The names of duty roles that grant access to subject areas include the words Transaction Analysis Duty (for example, Sales Managerial Transaction Analysis Duty). Access to a subject area is needed to run or create reports for that subject area.

### Catalog Folders

Catalog folders are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Sales Managerial Transaction Analysis Duty can access both the Sales Manager folder in the Catalog and the Sales Manager subject areas.

### Reports

Analyses are secured based on the folders in which they're stored. If you haven't secured reports using the report permissions, then they're secured at the folder level by default. You can set permissions against folders and reports for roles, catalog groups, or users.

### Information about Security and Reporting

When you receive your sales application, access to its functionality and data is secured using role-based access control. For more information about creating and securing reports, see the following guides on the Oracle Help Center at http://docs.oracle.com:

- Security Reference for Sales and Fusion Service

  Describes the sales application security reference implementation and includes descriptions of all the predefined data that is included in the security reference implementation for an offering.
- Creating and Administering Analytics for Sales and Fusion Service

  Explains how to view and work with analytics and reports.

- Subject Areas for Transactional Business Intelligence in Sales and Fusion Service

  Provides information about each subject area and the job roles and duty roles that secure access to the subject area.

*Related Topics*

- Security Reference for Sales and Fusion Service
- Creating and Administering Analytics for Sales and Fusion Service
- Subject Areas for Transactional Business Intelligence in Sales and Fusion Service

# Permissions for Catalog Objects

The Business Intelligence Catalog stores business intelligence objects such as dashboards, dashboard pages, folders, and analyses. Users can view only the objects for which they're authorized.

Note that the owner of an object or folder can't automatically access the object or folder. To access an object or folder, the user must have the proper permission assigned in the object or folder's permission dialog.

## What Are Permissions?

An object's owner or a user who has been given the proper privileges and permissions can assign permissions to catalog objects. Permissions are authorizations that you grant to a user or role to perform a specific action or group of actions on a catalog object. For example, if you work in the sales department and created a dashboard that contains quarterly sales projections, then you can give read access to this dashboard to all sales people, but give read, write, and delete access to sales directors and vice presidents.

> **Note:** Permissions are a part of the Oracle BI EE security model, and how permissions are initially assigned is based on how users, roles, and groups were set up on your application, and which privileges the Oracle BI EE administrator granted those users, roles, and groups.

## Permission Definitions

To control access to objects (such as a folder in the catalog or a section in a dashboard), you assign permissions to roles, catalog groups, and users. The permissions that you can assign vary depending on the type of object with which you are working.

The following table shows the main types of permissions encountered for sales users:

| Permission | Definition |
|---|---|
| Full Control | Use this option to give authority to perform all tasks (modify and delete, for example) on the object. |
| Modify | Use this option to give authority to read, write, and delete the object. |
| Traverse | Use this option to give authority to access objects within the selected folder when the user does not have permission to the selected folder. Access to these objects is required when the objects in the |

| Permission | Definition |
|---|---|
| | folder, such as analyses, are embedded in a dashboard or Oracle WebCenter Portal application page that the user has permission to access.<br><br>For example, if you grant users the Traverse permission to the /Shared Folders/Test folder, then they can access objects, through the BI Presentation Catalog or embedded in dashboards or Oracle WebCenter Portal application pages, stored in the/Shared Folders/Test folder and stored in sub-folders, such as the /Shared Folders/Test/Guest folder. However, users cannot access (meaning view, expand, or browse) the folder and sub-folders from the Catalog. |
| Open | Use this option to give authority to access, but not modify, the object. If you are working with an Oracle BI Publisher object, this option enables you to traverse the folder that contains the object. |
| No Access | Use this option to deny access to the object. Explicitly denying access takes precedence over any other permission. |
| Custom | Use this option to display the Custom Permissions dialog, where you grant read, write, execute, and delete permissions. |

For additional information about catalog object permissions, see Creating Analyses and Dashboards in Oracle Transactional Business Intelligence on Oracle Help Center at http://docs.oracle.com/.

# Transaction Analysis Duty Roles

Oracle Transactional Business Intelligence secures reporting objects and data through a set of delivered OTBI Transactional Analysis Duty roles. These duty roles control which subject areas and analyses a user can access and what data a user can see in the application.

These are some of the OTBI Transactional Analysis Duty roles used in the sales application:

- Partner Channel Transaction Analysis Duty
- Partner Channel Administrative Transaction Analysis Duty
- Sales Administrative Transaction Analysis Duty
- Sales Executive Transaction Analysis Duty
- Sales Managerial Transaction Analysis Duty
- Sales Transaction Analysis Duty
- Incentive Compensation Transaction Analysis Duty

This table lists analytics and reports available to sales users. It also shows the predefined job roles that can access the different analytics and reports, and the OTBI Transactional Analysis Duty roles that provide the access.

| Analytic or Report Name | Job Role | OTBI Transactional Analysis Duty Role |
|---|---|---|
| • Forecast vs. Quota<br>• Sales Stage by Age | Sales VP | Sales Executive Transaction Analysis Duty |

| Analytic or Report Name | Job Role | OTBI Transactional Analysis Duty Role |
|---|---|---|
| • Sales Performance Trend<br>• Top Open Opportunities | | |
| • Forecast Vs Open Pipeline: My Team<br>• My Team's Activities (By Type)<br>• My Team's Leads<br>• My Team's Performance<br>• My Team's Pipeline<br>• My Team's Tasks on Open Opportunities<br>• My Team's Top Open Opportunities<br>• Team Leadership Board<br>• Top Accounts by My Team's Activities | Sales Manager | Sales Managerial Transaction Analysis Duty |
| • My Open Leads by Age<br>• My Top Open Opportunities<br>• My Forecast vs. Open Pipeline<br>• My Open Leads by Source<br>• My Open Tasks<br>• My Performance<br>• My Pipeline<br>• My Stalled Opportunities<br>• My Top Accounts by Open Opportunities<br>• My Unaccepted Leads by Age<br>• My Won Opportunities<br>• Top Accounts by My Activities | Sales Representative | Sales Transaction Analysis Duty |
| • Evaluating My Partners' Pipeline<br>• Evaluating My Partners' Quarterly and Yearly Closed Revenue<br>• Evaluating My Partners' Current Quarterly Sales<br>• Evaluating My Partners' Win Rate | Channel Account Manager | Partner Channel Transaction Analysis Duty |

**Note:** The predefined Transaction Analysis Duty roles provide permissions to view but not create analyses and reports. Permissions to create reports are assigned at the job role level using Business Intelligence roles.

For additional information about the job roles that secure access to sales and service subject areas, and the OTBI Transactional Analysis Duty roles assigned to each job role, see the guide Subject Areas for Transactional Business Intelligence in Sales and Fusion Service.

# Business Intelligence Roles

Business Intelligence roles grant access to analytics functionality, such as the ability to run or author reports. Assign users one or more of these roles, in addition to roles that grant access to reports, subject areas, catalog folders, and sales data.

Business Intelligence roles apply to both Oracle Analytics Publisher and Oracle Transactional Business Intelligence (OTBI).

These are the Business Intelligence roles.

| Business Intelligence Role | Description |
|---|---|
| BI Consumer Role | Runs Business Intelligence reports. |
| BI Author Role | Creates and edits reports. |
| BI Administrator Role | Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on. |
| BI Publisher Data Model Developer Role | Creates and edits data models. |

## BI Consumer Role

The predefined OTBI Transaction Analysis Duty roles inherit the BI Consumer Role. You can configure custom roles to inherit BI Consumer Role so that they can run reports but not author them.

## BI Author Role

BI Author Role inherits BI Consumer Role. Users with BI Author Role can create, edit, and run OTBI reports. All predefined sales job roles that inherit an OTBI Transaction Analysis Duty role are also assigned the BI Author Role at the job role level, except for the Sales Representative job role which isn't assigned the BI Author role.

## BI Administrator Role

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role. The predefined sales and service job roles don't have BI Administrator Role access.

## BI Publisher Data Model Developer Role

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Users with either of these predefined job roles can manage BI Publisher data models.

# Configure Security for Oracle Transactional Business Intelligence

Oracle Transactional Business Intelligence secures reporting objects and data through the following types of roles:

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles, for example, Sales Managerial Transaction Analysis Duty. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.
- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to functionality such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports and subject areas to create and run reports and view analytics.

You can't copy or modify the Business Intelligence roles or the Transaction Analysis Duty roles provided with the application, or the associated security privileges. You also can't copy any role with a role code prefix of OBIA, for example, Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS_GENERIC_DUTY). But you can configure reporting security according to your security requirements as described here.

## Modifying Transaction Analysis Duty Role Assignments

If you want to change the subject areas that users have access to, then create a job role and provide the custom role with the Oracle Transactional Business Intelligence duty roles that provide the required access.

For example, you can create a role that provides access to both partner and sales team subject areas by assigning both the Sales Managerial Transaction Analysis Duty and the Partner Channel Transaction Analysis Duty to the custom role.

## Modifying Business Intelligence Role Assignments

The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle Analytics Publisher. The default Business Intelligence roles used in the sales application are BI Consumer and BI Author.

The delivered Transaction Analysis Duty roles inherit the BI Consumer Role, which provides view-only access to analyses and reports. You assign the BI Author Role at the job role level, giving you flexibility in granting the BI Author privilege to only those job roles that you want to have access to create and edit analyses and reports.

All predefined sales job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default, except for the Sales Representative job role. However, you can optionally create copies of the predefined job roles and add or remove the BI Author Role from the custom roles as required. You can also add the BI Administrator Role to custom job roles if you have users who need to be able to perform high-level tasks in Business Intelligence, such as work with catalog groups.

*Related Topics*

- BI Administrator Permissions

# View Reporting Roles

Viewing reporting roles can help you to understand Oracle Transactional Business Intelligence security. This topic explains how to view the following:

- The reporting roles that a job role inherits
- The reporting roles you are assigned

## View the Reporting Roles Assigned to a Job Role

To view the OTBI reporting roles that a job role inherits, perform the following steps:

1. Sign in to the application with the IT Security Manager job role.
2. Select **Navigator** > **Tools** > **Security Console**.
3. On the Security Console, search for and select a job role. For example, search for the Sales Manager job role.

   Depending on the enterprise setting, either a graphical or a tabular representation of the role appears. Switch to the tabular view if it doesn't appear by default.
4. Notice that the Sales Manager job role inherits the BI Author Role directly. The Sales Manager job role also inherits a number of Transaction Analysis Duty roles, such as the Sales Managerial Transaction Analysis Duty role and the Marketing Lead Transaction Analysis Duty role.
5. Click the Show Graph icon to switch to a graphical view of the Sales Manager job role.
6. Locate and expand one of the OTBI roles, for example, expand the Sales Managerial Transaction Analysis Duty role.

   Notice that the role inherits the BI Consumer Role. It also inherits the Transactional Analysis Duty role which is required to run queries and reports.

## View the Reporting Roles You Are Assigned

To view all of the duty roles that you are assigned, including Business Intelligence roles and Transaction Analysis Duty roles, perform the following steps:

1. Select **Navigator** > **Tools** > **Reports and Analytics** to open the Reports and Analytics work area.
2. Click the **Browse Catalog** button.

   The Catalog page opens.
3. Click your user name in the global header, then select **My Account**.
4. Click the Application Roles tab.

   All the duty roles you are assigned are listed, including Transaction Analysis Duty roles and Business Intelligence roles.
5. Click **OK** to return to the Catalog page.
6. Click **Sign Out** to return to the Oracle Applications Cloud window.

# Display Direct Report Data in Participant Manager Reports

This topic applies only to Incentive Compensation. You must enable the Secure by Manager Hierarchy person security profile before participant managers can see direct report participant data in their business intelligence reports. The application automatically generates and associates data grants using this security profile.

In the Setup and Maintenance work area:

1. Add the security profile.
2. Refresh the manager hierarchy.

## Add the Security Profile

Only users with either View All HCM Data or IT Security access can do these steps.

1. In the setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Data Role and Security Profiles
2. Search for roles staring with **Incentive**.
3. In the Search Results section, select **Incentive Compensation Participant Manager**.
4. On the toolbar, click **Assign** to open the Assign Data Role: Role Details page.
5. Click **Next** to open the Security Criteria page.
6. In the Person Security Profile field, select **View Manager Hierarchy**.
7. Click the **Secure by Manager** check box if it isn't already selected.
8. Click **Review**.
9. Click **Submit** to return to the Manage Data Role and Security Profiles page.
10. Click **Done** to return to the All Tasks tab.

## Refresh the Manager Hierarchy

You must run and schedule the Refresh Manager Hierarchy process to populate the HR Foundation Person tables with the manager hierarchy information. Reporting data is unavailable until you run the process.

1. On the Navigator menu within Tools, select **Scheduled Processes**.
2. On the Search Results section toolbar, click **Schedule New Process**.
3. In the **Name** field, search for and select **Refresh Manager Hierarchy**.
4. Click **OK** to return to Schedule New Process.
5. Click **OK** to open Process Details.
6. Click **Submit**, which causes the Confirmation to appear.
7. Click **OK** to return to Process Details.
8. Click **Cancel** to return to the Overview page.

# FAQs for Security and Reporting

## Can I configure Oracle Transactional Business Intelligence duty roles?

You can't modify the predefined OTBI duty roles or the associated security privileges. But you can configure Oracle Transactional Business Intelligence reporting security by assigning different OTBI duty roles to a custom job role if necessary.

# 6 Configure and Troubleshoot Data Security

## Overview of Data Security Configuration

Learn some of the ways you can configure and troubleshoot data security for sales and service users by reviewing the information in this chapter.

How sales database resources are secured in your environment depends on when you were provisioned with the sales and service application:

- If you started using the sales application before release 22B, then the database resources of your enterprise are secured using data security policies, which are assigned to job roles. Data security policies specify the roles that can perform a specified action on an object and the conditions under which the action can be carried out.

  > **Note:** If you've configured one or more access groups or object sharing rules, your users receive data access through a combination of data security policies and access group rules.

- If you're using the sales application for the first time in release 22B or later, your database resources are secured using system access groups and rules. When you assign job roles to users, they're automatically assigned membership of an associated system access group, and receive all the data permissions provided by the access group object sharing rules. These rules specify the access groups that can perform a specified action on an object, and the conditions under which the action can be carried out.

The conditions specified in both data security policies and access group rules control visibility to record-level data associated with a business object, such as an opportunity. Conditions can use a number of components, such as team or territory access, as mechanisms for sharing data. The scope of visibility varies by object, and multiple visibility levels are supported by an object for a role.

Regardless of whether your environment was provisioned with data security policies or system access groups rules, it's recommended that you use custom access groups to supplement the data access your users receive through their job role assignments.

The following table shows your options for reviewing, configuring, and troubleshooting data security.

| Work Area | What You Can Do | When to Use |
|---|---|---|
| Access Groups | From the Access Groups page you can configure data security by creating custom access groups, adding members to these groups, and defining rules to specify the access that group members should have to object data. | It's recommended that you use access groups and rules to configure data security. Access groups are easy to create and manage, and are processed more efficiently than data security policies.<br><br>**Note:** If you're using the sales application for the first time in release 22B or later, you have to use access groups to configure user access to object data. |
| Sales and Service Access Management | From the Sales and Service Access Management work area you can review and configure the data access provided by data security policies assigned to job roles. You can | Use this work area to get an overview of a user's access to data, to troubleshoot user access issues, and to review the data security policies assigned to job roles. |

| Work Area | What You Can Do | When to Use |
|---|---|---|
| | also review all a user's access to object data, whether from data security policies or access group rules. | |
| Security Console | From the Security Console, you can review and configure the access provided by the data security policies assigned to a role. You can also create database resources, and define custom conditions for a resource. | It's recommended that you use access groups and rules to configure data security when possible. But you can optionally use the Security Console to define database resources and custom conditions. You can also edit data security policies when creating, copying or editing roles on the Roles tab of the Security Console. |

**Note:** Data security changes made in any of the work areas described in the table are immediately available in all work areas.

Review this chapter for information about how to use the Sales and Service Access Management work area to configure data security, or for information about managing database resources and editing data security policies on the Security Console. For information about configuring access using access groups, see the Access Groups chapter in this guide.

# Sales and Service Access Management Work Area

As an IT Security administrator, you must be able to easily view the data a predefined role can access and to easily configure access to data for a user group using custom roles. Administrators must also be able to troubleshoot access issues for users.

You can perform all of these tasks using the Sales and Service Access Management work area, which provides simple interfaces where you can do these tasks:

- Create and manage access groups to provide sales resources with additional visibility to sales object data.

  See the Access Groups chapter for information about using access groups.
- Troubleshoot access issues for users:
  - Review all a user's access to object data, whether from data security policies or access groups
  - Identify the cause of any issues the user is experiencing in accessing specific records
- Review and configure the data access provided by roles:
  - View data access by object for a predefined Oracle CX role or for a custom role
  - Configure data security to add or remove a custom role's access to object data
  - End-date policies and configure advanced data permissions
  - Extend access to additional objects for custom roles

**Note:** You can view policies for custom objects in the Sales and Service Access Management work area but you can only configure security for custom objects in Application Composer.

## Access to the Sales and Service Access Management Work Area

The Manage Sales and Service Access privilege (ZCA_MANAGE_SALES_AND_SERVICE_ACCESS_PRIV) grants access to all the functionality in the Sales and Service Access Management work area. This privilege is assigned by default to the IT Security Manager and the Customer Relationship Management Application Administrator job roles.

Users assigned the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV) can access the Sales and Service Access Management work area to create and manage access groups. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege.

If necessary, you can provide access to all the work area, or to the Access Groups region of the work area, by granting the Manage Sales and Service Access functional privilege or the Manage Group Access functional privilege to a custom job role.

# Review and Configure Data Access for Roles

## Review a Role's Access to Object Data

You can review the visibility provided by job roles to object data by selecting the Manage Data Policies tab on the Sales and Service Access Management page. The Manage Data Policies page displays a read-only view of all the data security policies provided by a predefined or custom role for an object.

You can use this information to query existing policies so you can answer questions such as these:

- What's the most appropriate role to apply to a set of users?
- What's the most suitable role to copy when you need to extend the access provided by existing predefined roles?
- Why can't users access specific data?

By default, active policies are displayed for a role and object but you can also review inactive policies.

Here's how to review data access for a selected role and object:

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.

   > **Tip:** You can also access the Sales and Service Access Management page from the Setup and Maintenance work area by selecting the Manage Sales and Service Access task in the Users and Security functional area of the Sales offering.

3. On the Sales and Service Access Management page, click the Manage Data Policies tab.

   The Manage Data Policies page contains two areas: the Active Policies table, which lists each data policy for the selected object and role combination, and the Advanced Permissions table, which shows more detail about any advanced permissions available for a policy selected in the Access Policies table.

4. Select a role in the **Role** field.

   You can select either a custom or a predefined role. To search for a role:

   a. In the **Role** field drop-down list, click **Search**, then enter the role name in the **Role** field of the Role dialog box.
   b. Click **Search** again. From the search results, select the role you want, then click **OK**. Note that in the search results predefined roles are identified by a **Yes** in the Predefined role column.

5. Select an object in the **Object** field.

   The **Object** field lists all the sales and service objects the role can access.

   > **Note:** Select the Trading Community Party object to view access policies for both accounts and contacts.

6. Click **Find Policies**.

   The Active Policies table now lists all the active data security policies relating to the object you selected for the role you selected. You can view more or less information for the policies in the table by selecting the **Columns** option in the **View** menu.

   This information is shown for each active policy in the Access Policies table.

| Field | Value |
|---|---|
| Condition | Lists the condition that must exist for this data policy to take effect. For example, if you selected the Sales Representative role and the Opportunity object, the condition might state that this policy applies when the user assigned the Sales Representative role is an opportunity sales team member with edit or full access. |
| Permissions | Shows the access provided by the policy. For example, if the **Read**, **Update**, and **Delete** check boxes are selected, then this policy provides a user with read, update, and delete access to the object when the conditions specified in the policy are met, for example, when the user is an opportunity sales team member with edit or full access.<br><br>The **Advanced** field indicates the number of advanced permissions defined for the policy. Not all objects or policies have advanced permissions. |
| Start Date | Indicates the date when the policy was activated. |
| End Date | Indicates the date when the policy is deactivated. |
| Role Code<br><br>Role Name | Lists the role name and code of the role the policy is associated with. In most cases, the policy relates to the top-level job role you selected in the **Role** column, but in some cases, the policy is provided by an inherited duty role. A policy can even be provided by both the top-level role and by an inherited role. |
| Custom Condition | Indicates whether the condition specified in the policy is a predefined condition provided by Oracle or is a custom condition that you created previously. |

| Field | Value |
| --- | --- |
| | |

7. You can limit the policies that are shown for the role and object by clicking the **Query By Example** filter icon and entering filter text. You can filter by condition, role name, or role code.

   For example, currently the standard Sales Representative job role provides data visibility to all accounts and contacts. To view the conditions that are providing this full access, use these steps:

   a. Select **Sales Representative** in the Role field, **Trading Community Party** in the **Object** field, and click **Find Policies**.
   b. Click the **Query By Example** filter icon, and enter the text **All records** in the query field above the Condition column.

   The page is refreshed and displays two policies that provide all record access. Notice that one policy is provided by the Sales Representative role and the other by an inherited role, Contract View Access Across All Contracts. If you wanted to create a version of the Sales Representative role that had more restricted access to accounts and contacts, you would have to create custom copies of both roles and remove the All records policies from each.

   To remove the filter, click the **Clear All** icon in the query row.
8. To view the advanced permissions defined for a selected policy in the Access Policies table, scroll to the Advanced Permissions table.

   Advanced permissions provide a finer-grained method of controlling what the user can do. For example, a policy might provide update access to an opportunity but the advanced permission for the policy might allow you to restrict that update access to specific attributes.

   For each advanced permission, the Advanced Permissions table shows the type of access provided, for example, Read access, and the action it relates to, for example, View Opportunity.
9. If you want to view the inactive policies for a selected role and object on the Manage Data Policies page, select the **Inactive policies** check box.

   Inactive policies are policies that you set an end-date for and the end-date has passed. The number of inactive policies for the role and object is shown in parentheses beside the **Inactive policies** check box. For example, the number **1** indicates that there is only one inactive policy for the role-object combination.

# How do I edit the data access permissions for a custom role and an object?

You can update existing and future-dated policies for a custom role and object, and grant access to new subsets of data for the role, using the Active Policies edit page of the Sales and Service Access Management work area.

For example, you can:

- Add or remove all access to individual policies
- Configure read, update, and delete permissions for a specific policy
- End-date policies to inactivate them
- Configure advanced permissions for policies

Follow these steps to edit the permissions to object data for a custom role.

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.
3. On the Sales and Service Access Management page, click the Manage Data Policies tab.
4. Search for or select a role in the **Role** field.

   You can't edit policies on predefined roles, so search for and select a custom role. For example, if you copied the predefined Salesperson role to create a custom version of the role, you could select it.
5. Select an object in the **Object** field, for example, select the **Sales Lead** object.

   > **Note:** Select the Trading Community Party object to view access policies for both accounts and contacts.
6. Click **Find Policies**.
7. Click the **Edit** icon and the Active Policies edit page for the selected role and object is displayed.

   The Access Policies table shows all available policies for the selected role and object by default but you can use the **Show Conditions** filter to display only policies that are granted or only policies that aren't granted.
8. Configure the access provided to the selected object for the selected custom role by selecting or deselecting the **Read**, **Update**, or **Delete** checkboxes for a policy.

   For example, if you're editing policies for a custom Salesperson role and the Sales Lead object, you can perform data configuration tasks such as:

   - Restrict the ability to delete leads to lead owners by finding any policies that provide lead access to team members and deselecting the **Delete** checkbox for these policies.
   - Allow sales representatives to view retired leads by finding the policy that grants this access, then clicking the **Read** checkbox.
9. You can remove all access granted by a policy. For example, if your company doesn't use territory access, you can remove territory access to lead data using one of the following methods:

   - Review the Condition column to find the policies that grant territory access, then deselect the **Read**, **Update** and **Delete** checkboxes for each of these policies.
   - End-date the policies so that they're no longer active by selecting a date that has passed in the **End Date** field, for example, select yesterday's date.

   > **Note:** To reactivate a policy that's deactivated, reassign the appropriate read, update, and delete permissions to the relevant criteria and specify a start date for the policy.
10. If a policy has an advanced permission associated with it, then you can edit the advanced permission to specify more granular levels of access to the object.

    For example, a policy might provide full access to lead data for a resource in the territory assigned to the sales lead. You can restrict this access by selecting the policy, then scrolling to the Advanced Permissions table for the policy. You can remove update access to the lead data but retain read access by deselecting the **Update** checkboxes.

    > **Note:** You can update the advanced permissions for a policy only if the related permission in the parent row in the Access Policies table is checked. For example, if the read permission in the parent row of a policy isn't selected, none of the read permission options in the Advanced Permissions table can be edited.

11. Click **Save and Close**.

    Your changes are saved and the Manage Data Policies page is displayed where you can review your changes. If you've end-dated a policy, note that the number in parentheses beside the **Inactive policies** checkbox is incremented.

*Related Topics*

- How do I create and manage access groups?

# Considerations When Editing Inherited Roles

This topic describes some of the things to keep in mind when you edit inherited roles on the Active Policies page of the Sales and Service Access Management work area.

To add or remove a job role's access to object data, you have to know which policies provide the access. A job role can be assigned a policy in these ways:

- It can be assigned a policy directly
- It can inherit a policy indirectly from an inherited role
- It can receive the same policy from more than one role

The information on the Active Policies page lets you view all policies a job role is assigned, from all sources, for the selected object. For each policy in the Access Policies table, the **Role Name** field lists the role that the policy is associated with; this is either the top-level job role you selected on the Sales and Service Management page, or a duty role that the top-level role inherits.

You can't edit policies that are inherited from predefined duty roles because predefined roles can't be edited. But you can edit policies that are inherited from custom duty roles. If you edit a policy provided by an inherited custom duty role, keep in mind that if the custom duty role is also inherited, directly or indirectly, by other roles then the change you make to the policy also impacts these other roles.

To make sure that you don't inadvertently change the access provided by roles other than the top-level job role you're editing, a warning message alerts you if a policy change you're making impacts other roles. The message lists the names of all roles impacted by your edit, and prompts you to confirm whether or not you want to continue to make the change. Select one of these options:

- Click **Yes** to continue to apply the access change to the inherited custom role in either of these situations:
    - You want to make the access change to all the roles listed in the warning message.
    - You don't want to make the access change to all the roles listed in the warning message, but you do want to apply the access change to the job role you're editing now.

      In this situation, make a note of the roles listed in the message before clicking **Yes**. At a later time, you can directly update each role listed in the message to restore the access it provides to its original setting. This process can be time consuming if there are a number of roles affected by the edit of the inherited duty role so it's a good idea to avoid this situation if possible. For example, if you removed a privilege from the custom inherited role, you will have to manually add the privilege back to each job role listed in the message, or to the job role associated with each duty role listed in the message.

- Click **No** if you decide not to apply the access change to the inherited custom role. Instead, use these steps to implement the access change for the top-level job role only:
  a. Modify the role hierarchy of the top-level job role by removing the inherited custom role.
  b. Do one of the following:
     - Make a copy of the inherited custom duty role you removed using the **Copy top role** option, assign the copied duty role to the top-level job role, then edit the duty role as required.
     - Directly assign the job role with the access provided by the removed inherited duty role that you want to retain.

# Edit Inactive Policies

If you specified an end date for a policy, then once the end date is passed, the policy is inactive. You can't edit inactive policies for custom roles but you can delete them.

To delete an inactive policy:

1. On the Sales and Service Access Management page, click the Manage Data Policies tab.
2. Select a custom role in the **Role** field and an object in the **Object** field.
3. Click the **Inactive policies** checkbox.
4. Click **Find Policies**.

   All inactive policies are displayed in the Inactive Policies table.
5. Click the **Edit** icon.
6. On the Inactive Policies page, select a policy and click the **Delete** icon.
7. Click **Yes** when a warning is displayed.
8. Click **Save and Close** to return to the main page.

   The deleted policy is no longer included in the Inactive Policies table, and the number in parentheses beside the Inactive policies checkbox is reduced.

**Note:** You can reactivate a policy that's deactivated by reassigning the appropriate read, update, and delete permissions to the relevant criteria and specifying a start date for the policy on the Active Policies edit page.

# Extend Access to Additional Objects for a Custom Role

You can provide custom roles with visibility to object data they can't currently access by creating new data security policies on those roles for the relevant object.

For example, if you want to provide sales managers with access to subscription account data for a specific initiative, then you have to create access to the relevant subscription account object for a custom version of the Sales Manager job role, because the Sales Manager job role doesn't provide access to this data by default.

To create access to a new object for a custom role:

1. On the Sales and Service Access Management page, click the Manage Data Policies tab.
2. Click the **Create** button.
3. On the Create Policies page, search for the custom role whose access you want to extend in the **Role** field.

4. Select the object you want to provide access to in the **Object** field.

   For example, select the object for subscription accounts, **Subscription Account**. The only objects available for selection are objects where data security policies are not already defined for the custom role.
5. Click **Find Policies**.

   All the data security policies defined for the selected object are displayed in the Access Policies table. There are no permissions selected in the Permissions columns because data access to the object hasn't previously been configured for the custom role you selected.
6. Locate the condition that provides the data access you want to implement for the object.

   For example, if you want to provide the custom sales manager role with read access to all subscription account records, use these steps:

   a. Locate the condition that provides the required access. In this example, locate the condition: **Access the subscription account for table ATC_SUBSCR_ACCOUNTS for all subscription accounts**.
   b. Click the **Read** check box for this condition.
   c. Specify a **Start Date** of today and an appropriate **End Date**.
7. Click **Save and Close**.

   On the Manage Data Policies page, the new policies you added are now listed in the Active Policies table for the role and object.

   > **Note:** You can view data security for custom objects using the Sales and Service Access Management work area, but you can only edit security policies for custom objects using Application Composer.

# Review and Troubleshoot Data Access Issues for Users

## Overview of the Data Access Explorer

You can use the access explorer functionality in the Sales and Service Access Management work area to quickly troubleshoot data access issues reported by your users. These are some examples of the typical access issues you might have to investigate:

- You create a custom sales representative role that removes access to all accounts but users assigned the custom role still have all account access. Which data access conditions or access group rules are providing the access?
- A sales manager can't see opportunities assigned to her reports. Which data access condition or access group rule must she be assigned to get access?

To identify the cause of a user access issue, you must be able to see all the access a user currently has to object data, whether from data security policies or access group rules, and all the policies or rules that provide access to the relevant object or record. You can view both types of information on the Explore UI. You can:

- Review all the access policies granted to a user for an object, and all the roles that provide the access.
- Review all the access group rules granted to a user for an object, and all the access groups that provide the access.
- Discover which data security policies and rules are affecting a user's ability to view a specific object record.

With this information, you can identify why a user can or can't view a specific record or records, and then grant or revoke the appropriate data access.

> **Note:** The Explore UI shows the data access users receive through the Oracle CX job and duty roles they're assigned. It doesn't show users access to object records provided by non-CX roles, such as Oracle HCM roles, that they might also be provisioned with.

# Access Group Rules and the Access Groups Enablement Data Security Policies

On the Explore UI, you can view a user's access to data from both access group rules and data security policies. This topic describes the interaction between access group rules and the policies provided by the Access Groups Enablement duty role.

To receive access to object records through access groups, the following conditions must be met:

- Users must be assigned the relevant active rules through their access group membership.
- Users must be assigned the appropriate data security policies provided by the Access Groups Enablement duty role.

  These data security policies are required for users to get the access to object data provided through access groups, but they don't provide access to object data themselves.

Users are automatically assigned the Access Groups Enablement duty role through the predefined or custom job roles they're assigned, or through the Resource abstract role. In general, for each object supported for access groups, the Access Groups Enablement duty provides users with data security policies for each access level supported by the object; usually read, update, delete, and full access.

When reviewing information on the Explore UI, keep in mind that although users are assigned the Access Groups Enablement data security policies, they only receive the relevant data access if they're also assigned a corresponding active rule that provides the same access.

# Review a User's Access to Object Data

You can view all the access group rules and data security policies that currently affect the visibility a user has to an object, and the names of all the access groups and roles (Oracle CX roles or custom roles) that provide each rule or policy, using the access explorer.

Being able to identify all the access paths through which a user gains access to object records is essential when you want to remove a user's access to a set of data. Here's how to review all the policies and rules assigned to a user:

1. On the Sales and Service Access Management page, click **Explore Access**.
2. On the Explore page, select the name of the user whose access you're investigating in the **User Name** field.
3. Select an object from the **Object** field, for example, select the **Opportunity** object.

   Don't enter a value in the **Public Unique Identifier** field. You only enter a value in this field if you want to investigate a user's access to a specific record.
4. Click **Explore**.

The Access Groups and Data Security Policies tables are displayed showing all the active rules and policies that are granted to the user, providing you with an overall view of the user's access to data for the selected object. In each table, you can display more or less data for each rule or policy by selecting options from the **View** drop-down list for the table.

> **Note:** The Provides Record Access column in each table indicates if a policy provides access to the record specified in the **Public Unique Identifier** field. Because you haven't entered a value for this field, the Provides Record Access column is empty and the **Provides Record Access** drop-down list, which lets you filter values for the Provides Record Access column, is inactive.

- By default, the following information is displayed in the Access Groups table for each active rule the user is assigned through their access group membership.

| Field | Description |
|---|---|
| Status | The status of the rule. By default, active rules are displayed. A rule is active and provides the user with object access if the following conditions are met:<br>- The rule is active<br>- The rule is enabled for an access group the user is a member of<br>- The access group is active |
| Rule Name | The name of the rule that provides object access.<br><br>Provided you have the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV), you can review or edit the rule by drilling down on the rule name link. The access group Object Sharing Rules page is displayed allowing you to edit the rule in the context of an access group. See the Access Groups chapter for additional information. |
| Permissions (Read, Update, Delete) | The object permissions provided by the rule. |
| Group Name and Number | The name and number of the access group that provides the rule.<br><br>Provided you have the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV), you can review or edit the group by drilling down on the group name link. The access group Edit Access Group page is displayed allowing you to edit the group in the context of an access group. See the Access Groups chapter for additional information. |

- Data Security Policies and Advanced Permissions tables.

  By default, the following information is displayed in the Data Security Policies table for each active policy the user is assigned, either directly or indirectly. The advanced permissions defined for a selected policy in the Data Security Policies table are shown in the Advanced Permissions table.

| Field | Description |
|---|---|
| Status | The status of the policy. By default, active policies are displayed. |

| Field | Description |
|---|---|
| Condition | The condition that must be satisfied for the data security policy to take effect. |
| Permissions (Read, Update, Delete, Advanced) | The access provided by the policy. |
| Start Date<br><br>End Date | Indicates the policy activation start and end dates. |
| Role Name<br><br>Role Code | The name and code of the role that provides the policy. If the user inherits the policy from more than one role, click the link beside the role name to see a list of all roles. |
| Custom Condition | Indicates whether the condition is a predefined condition or a custom condition that you created. |

5. Once you have reviewed all the active policies or rules assigned to the user, you can select options from the **Show Access** drop-down list (Access Groups table) or the **Show Conditions** drop-down list (Data Security Policies table) to view rules and policies available for the object that the user isn't assigned or isn't receiving access from.

   For example, a user might be assigned a rule through group membership, but if the group isn't active, the user doesn't receive the access provided by the rule. Using these options can help you identify both gaps in a user's data access, and access a user doesn't require.

   This table shows the options available.

| Filter Option | Description ( Data Security Policies Table) | Description (Access Groups Table) |
|---|---|---|
| All | Display all policies defined for the object, including policies that are granted to the user and policies that aren't granted. | Display all rules that are defined for the object, including rules that are granted to the user and rules that aren't granted. |
| Granted and active | Display all active policies for the object that are granted to the user. This is the default value. | Display all active rules the user is assigned. |
| Granted and inactive | Display all inactive policies defined for the object that are granted to the user. | Display any rule that the user is assigned where the rule is inactive, where the group associated with the rule is inactive, or where the rule isn't enabled for the group. |
| Granted and future dated | Display all inactive policies defined for the object that are granted to the user which | Not applicable to rules. |

| Filter Option | Description ( Data Security Policies Table) | Description (Access Groups Table) |
|---|---|---|
| | are set to become active at some date in the future. | |
| Not granted | Display all policies defined for the object that aren't currently granted to the user. | Display any rule that provides object access that isn't granted to the user through access group membership. |

# How do I troubleshoot user access issues?

Troubleshoot data access issues for users using the access explorer.

On the Explore page, you can view all the access group rules and data security policies that affect a user's ability to view an object record and see whether or not each rule or policy has been granted to the user. You can use this information to find answers to questions such as these:

- What access policy do I have to grant to give the user access to a specific record?
- Which granted rule do I have to remove from the user so that the user can no longer access a record?

> **Note:** The Explore UI shows the data access users receive through the Oracle CX roles they're assigned. It doesn't show users access to object records provided by non-CX roles, such as Oracle HCM roles, that they might also be provisioned with.

To discover why there are issues with a user's access to a specific object record, you need to know:

- The user name of the user.
- The name of the object.
- The Public Unique Identifier (PUID) of the record.

  For information on how to find the PUID of a record, see the topic Display Public Unique Identifiers for Object Records.

  > **Note:** Some objects don't support PUIDs. You can't investigate a user's access to a specific record for these objects.

Use these steps to review all the rules and policies that affect a user's access to a specific object record.

1. On the Sales and Service Access Management page, click **Explore Access**.
2. On the Explore page, select the name of a user in the **User Name** field.
3. Select an object in the **Object** field.
4. Enter the PUID of the relevant record in the **Public Unique Identifier** field.

   The **Public Unique Identifier** field is unavailable if the object doesn't support public unique identifiers.

5. Click the **Explore** button.

   By default, all the rules and data security polices defined for the object that grant access to the record are listed in the Access Groups table and the Data Security Policies table respectively. Review the information in the **Status** column of each table to see which of these rules and policies the user is granted.

   > **Tip:** You can display additional data for each rule or policy by selecting options from the **View** menu of each table.

6. Select the information you're interested in viewing in each table.

   You can display different views of the user's access to the object record by changing the selections in the filters available for each table.

   For example, if a user can't access the record, it might be because the user isn't granted access to the record, or because the user is granted access but the relevant rule or policy is inactive, or because the relevant data security policy is future dated. Select these filter options to figure out the cause of the issue.

| Rules or Policies to View | Filter Options to Select |
|---|---|
| All the rules or policies that provide record access that the user isn't assigned | ○ **Not granted** option from the **Show Access** list (Access Groups table) or the **Show Conditions** list (Data Security Policies table)<br>○ **Yes** option from the **Provides Record Access** list |
| All the inactive rules or policies assigned to the user that provide record access | ○ **Granted and inactive** option from the **Show Access** list or the **Show Conditions** list<br>○ **Yes** option from the **Provides Record Access** list |
| All the future dated policies assigned to the user that provide record access | ○ **Granted and future dated** option from the **Show Conditions** list<br>○ **Yes** option from the **Provides Record Access** list |

7. In the Access Groups table, you can review the following information for each rule.

| Field | Description |
|---|---|
| Status | This field can have one of these values:<br>○ **Active**. The rule is granted to the user, the rule is active, and the rule is enabled for an active access group.<br>○ **Inactive**. The rule is granted to the user but the rule is inactive, the access group the rule is associated with is inactive, or the rule to group association is disabled.<br>○ **Not granted**. The user isn't granted the rule. |
| Provides Record Access | This field indicates if a rule grants access to the record specified in the **Public Unique Identifier** field. A check mark indicates that the rule provides record access; if the field is empty, the rule doesn't provide access to the record. |

| Field | Description |
|---|---|
| | In the Access Groups table, this field can also be set to **Not Applicable**. This value is displayed for inactive custom rules. You must activate custom rules to see whether or not they provide record access. |
| Rule Name and Group Name | For rules that are granted to the user, these fields show the name of the rule and the name of the access group through which the user is assigned the rule. For rules that aren't granted to the user, only the rule name is shown.<br><br>**Tip:**<br>You can click the **Rule Name** or **Group Name** fields to drill down to the edit rule or edit group pages on the Access Groups UI if you have the Manage Group Access privilege ( ZCA_MANAGE_GROUP_ACCESS_PRIV). This is useful if, for example, you want to investigate why a rule is inactive, or if you want to change the activation status of a rule.<br><br>See the Access Groups chapter for information about editing access groups and rules. |
| Permissions | For rules that are granted to the user, you can review the type of access provided by the rule. |

8. In the Data Security Policies table, you can review the following information for each policy.

| Field | Description |
|---|---|
| Status | This field can have one of these values:<br><br>- **Active**. The policy is active and is granted to the user.<br>- **Inactive**. The policy is granted to the user but is inactive.<br>- **Future dated**. The policy is granted to the user but the policy **Start Date** is set to a date in the future so the policy isn't yet active.<br>- **Not granted**. The user isn't granted the policy. |
| Provides Record Access | This field indicates if a policy grants access to the record specified in the **Public Unique Identifier** field. A check mark indicates that the rule provides record access; if the field is empty, the rule doesn't provide access to the record. |
| Role | The name of the role or roles that provide the policy. The role name is displayed only for policies that are granted to the user. |
| Permissions | For policies that are granted to the user, you can review the type of access provided by the policy. |

| Field | Description |
| --- | --- |
| | |

You can use the information from the **Status** and **Provides Record Access** fields to figure out what you have to do to provide a user with record access or to remove record access. But you can't edit data security policies on the Explore page.

For example, you might find that a policy that provides a sales manager with access to their subordinates opportunity records is future dated. In this case, note the name of the role providing the policy and edit the role on the Manage Data Policies page or on the Security Console to change the **Start Date** of the policy to the current date.

# Display Public Unique Identifiers for Object Records

The sales application generates a unique number (ID) for each business object record when the record is created. As an administrator, you can configure this ID to make it more user-friendly and readable. This user-friendly value is called the public unique ID (PUID).

**Note:** Not all objects support public unique IDs.

The PUID values for object records aren't displayed on the UI by default. To make these values visible, add the PUID field of the object to the object page using Application Composer. To do this, you require read-only access to all of the object records and access to Application Composer.

The following are the steps to add the **Opportunity Number** field to the Opportunities page. The **Opportunity Number** field displays the PUID value of opportunity records. Follow a similar process for any other objects whose PUID values you want to make available on the UI.

1. Activate a sandbox.

   See the topic Create and Activate Sandboxes for more information.
2. Select **Navigator** > **Configuration** > **Application Composer**.
3. On the Application Composer Overview page, navigate to the standard object whose PUID values you want to expose.

   For example, expand **Opportunity**
4. Select the **Pages** node.
5. Select the Application Pages tab.

   You can use the links on the tab to navigate to the object's configuration pages, where you can modify the pages that are available for the selected object. You can show or hide fields, rearrange fields, and add your own fields.
6. The **Opportunity Number** field shows the PUID value for an opportunity record. To make this field available on the UI, in the Landing Page Layouts region, select Standard Layout, then select **Duplicate** from the **Actions** menu.
7. Enter a name for the new layout, then click **Save and Edit**.
8. Locate the Fuse Opportunity Overview Table area and click the **Edit** icon.
9. In the Available Fields list, locate the **Opportunity Number** field and move it to the Selected Fields list.
10. Click **Save and Close**.

11. Test the changes by navigating to the Opportunities page as a user with access to the opportunities pages, for example, a salesperson.
12. Search for an opportunity, and verify that the PUID value is showing for the opportunity.
13. Publish the sandbox.
14. Navigate to the **Sales** > **Opportunities** page and search for an opportunity record. The PUID of the opportunity is displayed.

For information on exposing attributes and working with sandboxes, see the Configuring Applications Using Application Composer guide. For information on public unique IDs, see the sales Implementation Reference guide.

## PUID Fields for Objects

This table shows the field that must be exposed in Application Composer to make the PUID values for the object's records visible on the UI.

| Object Name in Application Composer | PUID Field to Expose |
|---|---|
| Account | Registry ID |
| Activity | Activity Number |
| Asset | Asset Number |
| Business Plans | Number |
| Campaigns | Campaign Number |
| Contact | Registry ID |
| Deal Registration | Registration Number |
| Deal Registration: Deal Products | DealProdNumber |
| Deal Registration: Deal Resources | DealResourceNumber |
| MDF Budget | Code |
| MDF Claim | Code |
| MDF Claim Settlement | Code |
| MDF Request | Code |
| Objective | Number |
| Opportunity | Opportunity Number |

| Object Name in Application Composer | PUID Field to Expose |
|---|---|
| Partner | Partner Number |
| Partner Programs | Program Number |
| Program Enrollments | Enrollment Number |
| Sales Lead | Lead Number |
| Sales Orders | Quote or Order Number |
| Sales Territory | Territory Number |
| Sales Territory Proposal | Proposal Number |
| Service Request | Reference Number |
| Subscription | Subscription Number |
| Work Order | Reference Number |

*Related Topics*

- Configuring Applications Using Application Composer
- Implementation Reference
- Create and Activate Sandboxes

# Why can't my ERP users access Sales and Service data?

Oracle's ERP roles don't give the same access as Sales and Service roles. Analyze your user's needs and give the appropriate roles to the Sales or Service user.

See the related topics for more information.

*Related Topics*

- Review a User's Access to Object Data
- How do I troubleshoot user access issues?
- Types of Sales Users

# Edit Data Security Policies on the Security Console

This topic describes how to edit data security policies when creating, copying or editing roles on the Roles tab of the Security Console.

> **Note:** You can also use the Sales and Service Access Management work area to review and edit the data security policies assigned to job roles.

## Edit Data Security Policies for Roles

To create a role, it's recommended that you copy a predefined role rather than create a role from scratch. In this case, your role automatically has the data security policies of the copied role. You can edit or remove the copied data security policies if necessary.

To edit or remove a data security policy for a copied role:

1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.

   The Edit Role: Basic Information page is displayed.
3. Click the Data Security Policies train stop.
4. On the Edit Role: Data Security Policies page, locate the policy then click the down arrow at the end of the policy row to show the actions menu.
5. Select one of the options listed:
   - To remove the policy, select the **Remove Data Security Policy** option.

     The policy is removed from the role.
   - To edit the policy, do the following:
     i. Select the **Edit Data Security Policy** option.

        The Edit Data Security Policy dialog box is displayed.
     ii. Change the values as required, for example, you can change the start date, the data set, or the action specified for the policy.
     iii. Click **OK** to save your changes, and close the confirmation message.

## Create Data Security Policies for Roles

You're unlikely to create data security policies unless you create roles from scratch. However, you can do so if required. Here are the steps to use.

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role's display name, role code, and role category.

   For additional information about creating roles, see the topic Create Job and Abstract Roles.
3. Click **Next**, then click **Next** again.
4. On the Create Role: Data Security Policies page, click **Create Data Security Policy**.

5. The Create Data Security Policy dialog box is displayed. A **Start Date** value is automatically assigned to the policy but can be changed.
6. In the **Policy Name** field, enter a policy name.

   The names of predefined data security policies begin with the words **Grant on**.
7. Search for and select the database resource for which you're defining the policy, for example, search for a table name.
8. In the **Data Set** field, select the subset of the data made available by the database resource the policy applies to.

   The following table describes the values you can choose for the Data Set field.

| Value | Description |
|---|---|
| Select by key | Use to limit the data set to a single record in the data resource. If you select this option, you must specify the primary key value that identifies the record in the database resource. |
| Select by instance set | Use to limit the data set to a subset of the data in the data resource. If you select this option, you must select a condition that defines a subset of the data. Conditions vary by resource.<br><br>If the predefined conditions available for a resource aren't appropriate, you can create custom conditions using access groups and rules. For information about access groups, see the Access Groups chapter. If you need additional help, contact Oracle Support. |
| All values | Use to include all data from the data resource in the data set. |

9. Complete the remaining fields, which depend on the selected combination of database resource and data set values.
10. In the **Actions** field, select the actions to which this data security policy applies.
11. Click **OK** to save the data security policy.

    You can view the new policy on the Data Security Policies page by scrolling to the end of the list of policies.

*Related Topics*

- Overview of Data Security Configuration
- Create Job and Abstract Roles

# Manage Database Resources

Data security policies secure your database resources. You can configure database resources if you want to define and secure a new database resource, or if the predefined data security conditions for a database resource don't meet your needs.

Using the Manage Database Resources and Policies page of the Security Console, you can:

- Define a new database resource
- Create data security policies to secure a new database resource

- Create database resource conditions for a database resource

To perform the tasks in this topic, you must have the IT Security Manager job role.

> **Note:** It's recommended that you use custom access groups to configure your users access to data whenever possible. Access groups provide better performance than custom data security policies and are easier to manage. Use the procedures in this topic to configure data security only if your requirements can't be achieved using access groups. For additional information about access groups, see the Access Groups chapter.

## Define Database Resources

A database resource is a database table or view that corresponds to a business object. When you create a custom business object that you want to secure, you must define its associated database table or view as a database resource. To define a table or view as a database resource, you must:

- Specify the primary key column of the database resource
- Filter columns of the database resource to exclude columns from being included in the row instance sets that can be made available to users through data security policies
- Identify conditions and actions for the database resource to determine what portions of the resource you can secure with data security policies and the operations that can be performed on the data

The following procedure describes each of these tasks.

To define a new database resource:

1. On the Security Console Administration tab, select the General subtab, then click **Manage Database Resources**.

   The Manage Database Resources and Policies page is displayed.
2. In the Search Results region, click the Create icon.

   The Create Database Resource page is displayed. The General Information subtab is selected by default.
3. Enter the values for the new database resource.

   The following table describes the field values to specify for the new database resource.

| Field | Value |
|---|---|
| Object Name | The name of the custom business object you want to define as a database resource. |
| Display Name | The display name of the business object. |
| Data Object | Select the data resource (table or view) that the custom business object represents.<br><br>When you select a value for the **Data Object** field, the Primary Key Columns and Filter Column Details areas are displayed. |
| Module | Select the user module associated with the resource. |

4. Click the **Function Security Enabled** check box if functional security policies have been defined for the business object.
5. In the Primary Key Columns area, click the Create icon.
6. In the **Primary Key** field, select the primary key column of the database table or view that the business object represents.
7. In the Filter Column Details area, select columns you want to exclude from the row instance sets defined by data security policies. The data from filtered columns isn't accessible by users. To select a column as a data filter, move it from the Available Columns list to the Selected Columns list.
8. Click the Condition subtab to create conditions for the new database resource, then click the Create icon.

   The **Create Database Resource Condition** dialog box is displayed. Conditions specify the rows of the database resource that can be secured by data security policies.
9. Create resource conditions as described in the procedure Creating Conditions for a Database Resource later in this topic.
10. Click the Action subtab.

    You define actions on the database resource to specify the operations data security policies can secure on a business object. For example, you can specify whether a user might have read, update, or delete access by naming actions for each of these and granting them in a data security policy to a particular role. An action must correspond with an operation that the business object implements.
11. Click the Add Row icon.
12. Enter a value in the **Name** and **Display Name** fields. The action name you enter must match an operation name defined for the corresponding business object. Actions act on the row instance sets specified by the database resource conditions that you define in a data security policy, that is, conditions determine the row instance set available to a user for a given action.

    You can specify more than one action.
13. Click **Submit**.
14. When the confirmation dialog box is displayed confirming that the database resource was created, click **OK**.

## Create Conditions for a Database Resource

Database resource conditions define what portions of a database resource can be secured by data security policies. You can't edit the predefined conditions provided by Oracle but you can create new conditions for a predefined database resource or for a database resource you've created.

A condition is a group of row instances that are determined by a simple XML filter or an SQL predicate (WHERE clause) that queries the attributes of the resource itself. You can define a condition to specify multiple row instance sets using an SQL WHERE clause with parameters. You don't need to define a condition for single row instance conditions (single value) or for all row instance conditions (all values). Both the single-value case and the all-values case can be easily defined when you create the data security policy.

> **CAUTION:** It's recommended that you avoid creating custom SQL predicates because they can have a negative impact on application performance. If you do use custom SQL predicates, you are responsible for creating and maintaining them yourself.

To create conditions for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.

   The Manage Database Resources and Policies page is displayed.

2. Search for the database resource whose conditions you want to edit.
3. In the Search Results list, select the appropriate database resource, then click the Edit icon.

   The Edit Data Security page is displayed.
4. Select the Condition subtab to define a new condition for the resource.

   Any existing conditions defined for the database resource are displayed. You can't delete or edit any predefined conditions.
5. Click the Create icon.

   The **Create Database Resource Condition** dialog box is displayed.
6. Enter a name and display name for the condition.
7. For the **Condition Type**, select one of the following:
   - Select **Filter** if you want to use the attribute picker to define a simple condition. If you select the filter condition type, you also must specify the following values:
     - For the **Match** option, select the **All** option if you want the filter conditions to include AND clauses or select the **Any** option if you want the filter conditions to include OR clauses.
     - In the Conditions area, click the Add icon.
     - Define the filter values.

       The following table describes the filter values for each field.

| Field | Value |
|---|---|
| Column Name | Select the column for which you're defining the filter. |
| Tree Operators | Select this option if the operator you want to use in the filter is a tree operator. |
| Operator | Choose the operator for the selected column filter. |
| Value | Enter a value as the test for the operator.<br><br>If you specified the Tree Operators option, click the Search icon. The **Select Tree Node** dialog box is displayed allowing you to choose the operator value. |

     - Click **Save**.
   - Select SQL Predicate if you know the attribute names of your condition and you want to use an SQL predicate consisting of a query on the table or view named by the database resource. Enter the SQL values in the **SQL Predicate** field.
8. Click **Save** to save the new condition.

## Create a Data Security Policy for a Database Resource

When you register a new business object as a database resource, users will initially be prevented from initiating the operations of the business object or from accessing the data of the resource. You define data security policies to make the data of a custom business object available to the users of the application.

Before you create a data security policy, make sure that the following tasks have been completed:

- Identify the business object that you want to secure and register its associated database table or view as a database resource.
- Identify and define any conditions that you want to make available for the database resource.
- Identify and register the actions that you want to secure for this database resource.

To create a policy for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.

   The Manage Database Resources and Policies page is displayed.
2. Search for the database resource that you want to secure by defining a policy.
3. In the Search Results list, select the database resource, then scroll down to the Policies Details area.

   All the policies defined for the database resource are displayed.
4. You can select an existing policy for editing by selecting the policy then clicking the Edit icon. In this case, however, click the Create icon to create a new policy.

   The **Create Policy** dialog box is displayed with the General subtab selected.
5. Specify the following information for the new policy:
   - In the **Name** field, enter a name for the policy.
   - In the **Start Date** field, enter the date on which the policy is to become active.

   The **Module** field is pre-filled with the name of the module associated with the database resource for which you're creating the policy but you can change this value.
6. Click the Role subtab, then click the Add icon to select the roles that are to be assigned the new policy.

   The **Select and Add: Roles** dialog box is displayed.
7. Select the roles to be assigned the new policy as follows:
   - In the **Role Name** field, enter the name of the role.
   - In the **Application** field, enter the application stripe of the role, for example, CRM, HCM, or FSCM, then click **Search**.
   - Select a role from the list of roles displayed, then click **Apply** to associate the role with the new policy.
   - Select any additional roles from the list and, when you have finished adding roles, click **OK**.

   All users assigned the roles you select are provided with access to the data defined in the policy.
8. Click the Rule subtab to define a rule to specify the rows of the database resource to which the policy applies.
9. Select one of the following values in the **Row Set** field:
   - To secure a specific row, select **Single Value**, then search for and select the row you want to secure in the **Row** field.
   - To secure all rows in the resource, select All Values.
   - To secure a subset of the data in the data resource select Multiple Values, then search for and select the condition that defines the subset of the data to be secured in the **Condition** field.
10. Click the Action subtab, then move actions from the Available Actions list to the Selected Actions list to specify the actions, applicable to the data secured on the database resource, which you want to grant to the role.
11. Click **Save and Close**.