Oracle Sales Cloud
Securing Oracle Sales Cloud
Release 8

April 2014
Contents

1 Understanding Oracle Sales Cloud Security

Securing Oracle Sales Cloud: Overview ................................................................. 1-1
Role-Based Security: Explained ........................................................................ 1-1
Predefined Sales Roles: Explained ................................................................. 1-2
Role Types: Explained ...................................................................................... 1-3
Duty Role Components: Explained ................................................................. 1-5
Role Inheritance: Explained ............................................................................ 1-6
How Users Gain Access to Opportunities: Explained .................................. 1-7
How Users Gain Access to Leads: Explained .................................................. 1-9
Security Customization: Points to Consider .................................................... 1-10
Reviewing Predefined Roles in the Security Reference Manuals: Explained .... 1-10

2 About Oracle Sales Cloud Users

Creating Users for Oracle Sales Cloud: Explained ........................................... 2-1
About Provisioning Enterprise Roles to Users: Explained ................................ 2-6
Creating Setup Users for Oracle Sales Cloud: Worked Example ..................... 2-8

3 Getting Ready to Create Application Users

What You Must Do Before Creating Application Users: Explained ................. 3-1
Creating Resource Organizations ...................................................................... 3-3
Designating a Resource Organization as the Top of the Sales Hierarchy ......... 3-4
Creating Additional Resource Roles ................................................................. 3-6
Creating Rules to Automatically Provision Enterprise Roles to Sales Users .......... 3-7
Setting Up E-Mail Notifications for New Users: Procedure ............................ 3-8

4 Creating Application Users

Creating Application Users for Oracle Sales Cloud: Worked Example ................ 4-1
Enabling Single Sign-On for Your Applications: Explained ............................ 4-3

5 Managing Application Users

Resetting User Passwords: Procedure ............................................................ 5-1
Changing User Resource Roles When Job Assignments Change: Procedure .... 5-2
Terminating User Accounts: Procedure .......................................................... 5-2
FAQs for Terminating Users ............................................................................ 5-4

6 Customizing Security
Security Customization: Overview ................................................................. 6-1
Recommendations for Customizing Security .................................................. 6-1
Creating a Custom Job or Abstract Role: Procedure ...................................... 6-2
Creating Custom Duty Roles: Procedure ....................................................... 6-4
Removing Create Account Functionality: Procedure ........................................ 6-6
Restricting Access to Sales Accounts: Worked Example ................................... 6-9

7 Synchronizing User and Role Information with Oracle Identity Management

Synchronization of User and Role Information with Oracle Identity Management: How It Is Processed ................................................................. 7-1
Scheduling the LDAP Daily Processes: Procedure ............................................. 7-2
Send Pending LDAP Requests: Explained ...................................................... 7-3
Retrieve Latest LDAP Changes: Explained ................................................... 7-4
Preface

This Preface introduces the guides, online help, and other information sources available to help you more effectively use Oracle Fusion Applications.

Oracle Fusion Applications Help

You can access Oracle Fusion Applications Help for the current page, section, activity, or task by clicking the help icon. The following figure depicts the help icon.

Note

If you don't see any help icons on your page, then click the Show Help icon button in the global area. However, not all pages have help icons.

You can add custom help files to replace or supplement the provided content. Each release update includes new help content to ensure you have access to the latest information. Patching does not affect your custom help content.

Oracle Fusion Applications Guides

Oracle Fusion Applications guides are a structured collection of the help topics, examples, and FAQs from the help system packaged for easy download and offline reference, and sequenced to facilitate learning. To access the guides, go to any page in Oracle Fusion Applications Help and select Documentation Library from the Navigator menu.

Guides are designed for specific audiences:

- **User Guides** address the tasks in one or more business processes. They are intended for users who perform these tasks, and managers looking for an overview of the business processes. They are organized by the business process activities and tasks.

- **Implementation Guides** address the tasks required to set up an offering, or selected features of an offering. They are intended for implementors. They are organized to follow the task list sequence of the offerings, as displayed within the Setup and Maintenance work area provided by Oracle Fusion Functional Setup Manager.

- **Concept Guides** explain the key concepts and decisions for a specific area of functionality. They are intended for decision makers, such as chief
financial officers, financial analysts, and implementation consultants. They are organized by the logical flow of features and functions.

- **Security Reference Manuals** describe the predefined data that is included in the security reference implementation for one offering. They are intended for implementors, security administrators, and auditors. They are organized by role.

These guides cover specific business processes and offerings. Common areas are addressed in the guides listed in the following table.

<table>
<thead>
<tr>
<th>Guide</th>
<th>Intended Audience</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common User Guide</td>
<td>All users</td>
<td>Explains tasks performed by most users.</td>
</tr>
<tr>
<td>Common Implementation Guide</td>
<td>Implementors</td>
<td>Explains tasks within the Define Common Applications Configuration task list, which is included in all offerings.</td>
</tr>
<tr>
<td>Functional Setup Manager User Guide</td>
<td>Implementors</td>
<td>Explains how to use Oracle Fusion Functional Setup Manager to plan, manage, and track your implementation projects, migrate setup data, and validate implementations.</td>
</tr>
</tbody>
</table>
| Technical Guides                   | System administrators, application developers, and technical members of implementation teams | Explain how to install, patch, administer, and customize Oracle Fusion Applications.  
**Note** Limited content applicable to Oracle Cloud implementations. |

For other guides, go to Oracle Technology Network at http://www.oracle.com/technetwork/indexes/documentation.

**Other Information Sources**

**My Oracle Support**

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.
Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications provides details on service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes.

In Oracle Fusion Applications, you can use Oracle Enterprise Repository at http://fusionappsoer.oracle.com for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww_grp@oracle.com. You can use Send Feedback to Oracle from the Settings and Actions menu in Oracle Fusion Applications Help.
Securing Oracle Sales Cloud: Overview

When you receive your Oracle Sales Cloud implementation, access to its functionality and data is secured using role-based access control (RBAC). This guide describes the RBAC controls provided by Oracle Sales Cloud, and describes the tasks you must perform to implement these controls so that users have appropriate access to Oracle Sales Cloud data and functions.

Some of the tasks described in this guide are performed only or mainly during implementation of Oracle Sales Cloud. Most, however, can be performed at any time and as new requirements emerge. During implementation, you can perform security-related tests:

- From an implementation project
- By opening the Setup and Maintenance work area (Navigator - Tools - Setup and Maintenance) and searching for the task on the All Tasks tab

Once the implementation is completed, you can perform most security-related tasks from the Setup and Maintenance work area. Any exceptions are identified in relevant topics.

Role-Based Security: Explained

Oracle Sales Cloud implements role-based access control (RBAC) to prevent unauthorized access to application resources. Users gain access to application functions and data when they are assigned enterprise roles, which correspond to their roles in your organization. Users can have any number of different roles, and this combination of roles determines the resources that the user can access. The job role providing the greatest level of access takes precedence.

Role-Based Access Control

Role-based security in Oracle Cloud applications controls who can do what on which set of data.

In role-based access:
### Component | Description
--- | ---
Who | This is a role assigned to a user, for example, the Sales Manager role.
What | This is a function that users with the role can perform, for example, approve sales forecasts.
Which Data | This is the set of data that users with the role can access when performing the function; for example, approve forecasts for salespersons who work for them.

Oracle Sales Cloud provides the following types of roles:
- Job roles
- Abstract roles
- Duty roles

You assign job and abstract roles directly to users using role provisioning rules. Duty roles are associated with job and abstract roles; they are not assigned directly to users.

### Predefined Sales Roles: Explained

Many job and abstract roles are predefined in Oracle Sales Cloud. You can assign each sales application user with one or more of the following job roles.
- Channel Account Manager
- Channel Administrator
- Channel Operations Manager
- Channel Partner Administrator
- Channel Sales Director
- Channel Sales Manager
- Customer Data Steward
- Data Steward Manager
- Master Data Management Application Administrator
- Partner Administrator
- Partner Sales Manager
- Partner Salesperson
- Sales Administrator
- Sales Manager
- Sales Vice President
- Sales Representative

These predefined roles are part of the Oracle Sales Cloud security reference implementation. The security reference implementation is a predefined set
of security definitions that you can use as supplied. Also included in the security reference implementation are roles that are common to all Oracle Cloud applications, such as:

- Application Implementation Consultant
- IT Security Manager

You must also assign the following abstract roles to all Oracle Sales Cloud users who are employees so they can carry out their work:

- Employee
- Resource

A complete list of all enterprise roles, and a detailed description of what access they provide, is included in Oracle Fusion Applications security reference manuals available in the Oracle Fusion Applications Technology Documentation Library (http://docs.oracle.com).

**Note**

To create users with implementation privileges, you must provision special enterprise roles. See the Creating Setup Users for the Oracle Sales Cloud: Worked Example topic and other user topics in this guide for more information.

### Role Types: Explained

This topic outlines the different types of roles defined in Oracle Sales Cloud, and describes their components.

#### The Components of Enterprise Roles

The following figure shows each of the role types and how they relate to one another.

![Diagram of role types](image)

**Note**
Abstract roles and job roles are also called enterprise roles or external roles because they are created in the LDAP directory and are not specific to an application pillar. Duty roles are also known as application roles because these roles are created in the Sales Cloud database and are specific to each Oracle application pillar.

- **Job roles**
  
  Job roles represent the job functions in your organization. Sales Representative and Sales Manager are examples of predefined job roles. You can also create custom job roles.

  Job roles provide users with the permissions they need to perform activities specific to their jobs. For example, providing a user with the Sales Manager job role permits the user to manage salespersons within the organization, follow up on leads, generate revenue within a territory, build a pipeline, manage territory forecasts, and assist salespeople in closing deals.

  You assign job roles directly to users.

- **Abstract roles**
  
  Abstract roles represent a worker’s role in the enterprise independently of the job they do. The following are examples of abstract roles used in Oracle Sales:

  - Employee
  - Resource
  - Contingent Worker

  You can also create custom abstract roles.

  Abstract roles permit users to perform functions that span across the different jobs in the enterprise. For example, users who are employees must be provisioned with the Employee abstract role, so they can update their employee profiles and pictures. For Oracle Sales Cloud, you must also provision users with the Resource abstract role, so they can work on leads, opportunities, and other sales tasks.

  You assign abstract roles directly to users.

- **Duty roles**
  
  Job and abstract roles permit users to carry out actions by virtue of the duty roles they include. Duty roles represent the individual duties that users perform as part of their job. They grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on.

  Job roles and abstract roles inherit duty roles. For example, the Sales Manager job role includes the Sales Lead Follow Up Duty and the Quota Management Duty. The Sales Lead Follow Up Duty makes it possible for the managers to work with leads. The Quota Management Duty enables the management of sales territory quotas.
Duty roles can also inherit other duty roles. They’re part of the security reference implementation, and are the building blocks of custom job and abstract roles. You can also create custom duty roles.

You don’t assign duty roles directly to users.

**Duty Role Components: Explained**

This topic describes the components that are associated with duty roles.

Duty roles are associated with two types of security policies: functional security policies and data security policies. Security policies define the privileges provided by the duty role to access specific application resources.

**Functional Policies**

Functional policies permit an individual who is assigned a duty role to access different user interface elements, Web services, tasks flows, and other functions. For example, a sales manager who has the Delete Opportunity functional policy will be able to view and click the Delete button. Removing that policy removes the button from view.

A functional policy is made up of the duty role name and the functional privilege (for example, Delete Opportunity) that specifies the application features that are being secured. 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 duty role. The name of the duty where it applies. For example, Opportunity Sales Manager Duty.
- A data privilege that defines the action being performed. For example, View Opportunity.
- The condition that must be met for access to be granted. For example, sales managers can view opportunities if they are in the management chain or are members of the sales team on the opportunity.

Each data security policy represents an underlying SQL query. The application evaluates the query at run time, and permits access to data that meets the condition. Data privileges are listed in the Data Security Policies section of the security reference manuals.

**Sharing Modes**

Data security policies specify conditions which control visibility to data associated with a schema object, such as an opportunity. Conditions can use the following components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

- Team membership
- Partner teams
• Territory
• Resource Hierarchy

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

Role Inheritance: Explained

Each role is a hierarchy of other roles:

• Job and abstract roles inherit duty roles.
• Duty roles can inherit other duty roles.

In addition, when you assign data and abstract roles to users, they inherit the data and functional security privileges associated with those roles.

Role Inheritance Example

This example shows how roles and privileges are inherited for a user assigned the Sales Manager job role.

The following figure shows a few representative duty roles. In reality, job and abstract roles inherit many duty roles, which themselves might inherit many duty roles.
In this example, the provisioning rule automatically provisions an employee sales manager with the enterprise roles needed to do the job: the Sales Manager job role, and the Employee and Resource abstract roles. Roles are inherited as follows:

- The Sales Manager job role inherits the Quota Viewing Duty and the Sales Manager Duty.

- Duty roles inherit other duty roles. For example, the Sales Manager Duty inherits many other duty roles including the Marketing Lead Analysis Duty and the Opportunity Sales Manager Duty.

- The duty roles are associated with functional security policies and data security policies. For example, the inherited Opportunity Sales Manager Duty has:
  - Functional security policies that specify which application pages and functions sales managers can access for deleting, assigning, closing, creating, and viewing an opportunity. The View Opportunity policy, for example, permits sales managers to view all UIs, Web services, and task flows related to opportunities.
  - Data security policies that specify the actions opportunity sales managers can perform on what opportunities and under what conditions.

For example, opportunity sales managers can view all data related to opportunities if they are an opportunity sales team member with view, edit, or full access.

**How Users Gain Access to Opportunities: Explained**

This topic explains how the security reference implementation provided by Oracle determines who can access what opportunity information in your sales organization.

Whether or not you can access a particular opportunity depends on your membership in the resource and territory hierarchies. You can access an opportunity if:

- You create the opportunity.
- You are on the opportunity sales team.
- You are the owner of the territory.
- The opportunity owner is your direct or indirect report in the resource hierarchy.
- If you are assigned to a territory for the sales account associated with the opportunity or if a territory is assigned to the revenue lines on the opportunity.

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 assigned to the sales account of the opportunity get read-only access to the opportunity and are not added to the opportunity sales team.

• Owners and members of territories assigned to the opportunity revenue 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 will always have full access.

The following figure illustrates some of the different ways you gain access to an opportunity:

• Named agents in the diagram (A, B, and C) can access the opportunity
• Unnamed agents (highlighted in yellow) cannot access the opportunity
• Sales managers can access the opportunity because a salesperson in their management chain has access.

This figure 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 are the initial owner.
• Agent B can access the opportunity because he is on the sales team.
• Agent C can access the opportunity because he is the owner of the NW territory.

• Sales managers who are higher up in the management chain can also see the opportunity because access is provided through the resource hierarchy. Agent C’s manager can access the opportunity information, but agent C’s colleagues cannot.

Note
Access using revenue lines and sales accounts are not shown in this figure.

Special Access
Some access is not affected by the management hierarchy and membership in sales teams or territories. This special access includes:

• Administrators: Administrators get access to opportunities and other objects. This access is based on their privileges, regardless of where the administrators are in the management hierarchy. Administrators do not have to be on the sales team or members of territories.

• Deal Protection: Salespersons assigned to an opportunity retain the sales credit on an opportunity even if they are moved to another opportunity.

• Team Selling: You can configure the application to allow salespersons to see all opportunities related to their sales accounts.

How Users Gain Access to Leads: Explained

This topic explains how the security reference implementation provided by Oracle determines who can access lead information in your sales organization.

Qualified leads are assigned to a sales team based on sales territories. Unqualified leads are assigned to individual lead qualifiers either manually or based on rules defined in the assignment manager engine. Whether or not you can access a particular lead depends on your membership in the resource and territory hierarchies.

You can access a lead if:

• You are the lead owner.

• The lead owner is your direct or indirect report in the resource hierarchy.

• You are a member of the lead sales team.

Resources in the management hierarchy of a newly added lead sales team member have the same level of access to the sales leads as the team member.

• You are the owner of the territory the lead is assigned to or of ancestor territories.

• You are a member of the sales territories assigned to the lead.
Note

Only the lead owner, or resources in the management chain of the lead owner, can change the lead owner.

Security Customization: Points to Consider

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 duties. If some business groups in your organization have the sales managers do forecasting, not the sales representatives, then you can create a custom Sales Representative role without those duties. Alternatively, if a predefined job role is too narrowly defined, then you can create a job role with a greater range of duties than its predefined equivalent.

During your implementation of Oracle Sales Cloud, you evaluate the predefined roles and decide whether changes are needed.

Tip

If you change the security reference implementation, then it is recommended that you create custom roles rather than modify predefined roles. For additional information, see the chapter Customizing Security later in the guide.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren’t represented in the security reference implementation, then you create a job or abstract role.

Predefined Roles with Different Duties

If the duties for a predefined job role don’t match the corresponding job in your enterprise, then you add duties to or subtract duties from the job role.

Predefined Roles with Missing Duties

If the duties for a job aren’t defined in the security reference implementation, then you create custom duty roles.

Reviewing Predefined Roles in the Security Reference Manuals: Explained

The Security Reference for Oracle Sales Cloud includes descriptions of all predefined security data in the Oracle Sales security reference implementation.
The Security Reference for Oracle Applications Cloud includes descriptions of all predefined security data that’s common to Oracle Fusion Applications.

You can access all information in these manuals from various Oracle Sales user interface pages. For example, you can review individual job roles using the Manage Job Roles task. However, using the manuals you can compare roles and plan any changes.

You can access the security reference manuals on cloud.oracle.com. Select Resources - Getting Started - Documentation - All Books.

Security Reference for Oracle Sales Cloud

The Security Reference for Oracle Sales Cloud contains a section for each predefined Sales job and abstract role. For each role, you can review its:

- Duties
- Role hierarchy
- Function security privileges

This information can help you to identify which users need each role and whether to make any changes before provisioning roles.
About Oracle Sales Cloud Users

Creating Users for Oracle Sales Cloud: Explained

This topic explains concepts that will help you create users for Oracle Sales Cloud.

User Types
When you sign up with Oracle Sales Cloud, you receive the user name and password for one initial user.
Sign in as the initial user to create other users. The following table explains the different types of users that you can create.

<table>
<thead>
<tr>
<th>Type of User</th>
<th>Description</th>
</tr>
</thead>
</table>
| Setup users      | When you provision users with the same enterprise roles as the initial user, they can perform all the standard implementation setups for your Oracle Sales Cloud implementation. These include managing security, enterprise setup, and creating other users, including other users with the same privileges. These enterprise roles are: Application Implementation Consultant job role  
IT Security Manager job role  
Application Diagnostic Administrator job role  
Employee abstract role  
Note  Even if setup users do not have the privileges to perform specialized tasks, they do have the privileges to assign themselves additional enterprise roles to make those tasks possible.  
Setup users are not created as resources in Oracle Sales Cloud and are not provisioned with the Resource abstract role. You cannot assign sales work to them and they cannot view sales transaction data or reports. |
<table>
<thead>
<tr>
<th>Type of User</th>
<th>Description</th>
</tr>
</thead>
</table>
| Sales administrators | Sales administrators are created as resources and provisioned with enterprise roles. The enterprise roles are based on their resource role, just like other application users.  
Because sales administrators are provisioned with the Sales Administrator job role, they have permission to manage the import of data from legacy systems, customize the application according to business needs, and create other application users.  
Unlike setup users, sales administrator users can view sales transactional data and reports. They cannot configure sales application security or perform tasks related to an enterprise setup.  
Sales administrator users are provisioned with the following enterprise roles:  
Sales Administrator job role  
Resource abstract role  
Employee abstract role  
To create sales administrators, follow the same procedure outlined in the Creating Application Users for Oracle Sales Cloud: Worked Example topic. |
| Application users   | Application users, such as sales managers and salespersons, can be created by both sales administrators and setup users.  
By entering resource information, you create application users as resources that can be assigned work and appear in your sales organization directory.  
Application users are provisioned according to their resource role. Their provisioned job roles do not permit them to perform implementation tasks, but they can perform a functional setup within the application, depending on their role.  
Application users are provisioned with:  
The job roles that they require to perform their job  
The Resource abstract role  
The Employee or the Contingent Worker abstract role, depending on the employee type of the user |
User Creation Methods

You can create users in one of the following ways. You can:

- Create users individually in the Manage Users work area. You can navigate to this work area using the Navigator menu from any application page.

  Use this method for creating all setup users and for creating application users unless the number of users that you are creating is large. For example, you may want to set up a small organization of test users that you can use to test your setups as you go along.

- Import users from a file using the File-Based Data Import group of tasks from the Setup and Maintenance work area.

  Import users from a file only if you have a large number of users to create. To import users, you must be prepared to spend some time understanding how user attributes are represented in Oracle Sales Cloud and how you will map the attributes in your file to the attributes required by the application. You cannot import setup users because the import process requires you to import sales resources.

See the Understanding File-Based Data Import: Getting Started and other help topics on file import.

Tasks You Accomplish by Creating Users

When you create users, you are accomplishing multiple tasks at the same time as outlined in the following table. Not all the tasks apply to setup users because they are not created as resources in the application.

<table>
<thead>
<tr>
<th>Task Accomplished</th>
<th>Oracle Sales Cloud Users (Including Sales Administrator Users)</th>
<th>Setup User</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send automatic e-mail notifications with the user names you entered and automatically generated temporary passwords.</td>
<td>Yes</td>
<td>Yes</td>
<td>The application sends the notifications to the user or to an administrator only once, either on creation or later, depending on the setup.</td>
</tr>
<tr>
<td>Automatically provision the enterprise roles that provide the security settings users need to do their jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>Enterprise roles are provisioned based on the autoprovisioning rules discussed in related security topics.</td>
</tr>
<tr>
<td>Create resources that can be assigned CRM work</td>
<td>Yes</td>
<td>No</td>
<td>Setup users are not resources in your application and so cannot be assigned to sales teams or view reports.</td>
</tr>
<tr>
<td>Task Accomplished</td>
<td>Oracle Sales Cloud Users (Including Sales Administrator Users)</td>
<td>Setup User</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create the resource reporting hierarchy used by Oracle Sales Cloud for reporting, forecasting, and work assignments</td>
<td>Yes</td>
<td>No</td>
<td>When you create a resource, you specify a manager for that resource and build a resource reporting hierarchy.</td>
</tr>
<tr>
<td>Create resource records that individual users can update with personal information to complete a directory of your organization</td>
<td>Yes</td>
<td>No</td>
<td>Setup users are not resources and so their information does not appear in your Sales directory.</td>
</tr>
<tr>
<td>Create a hierarchy of resource organizations</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Each resource is assigned to a resource organization, and the application builds a hierarchy of these organizations based on the resource reporting hierarchy. Setup users are not resources and so are not assigned to resource organizations.</td>
</tr>
<tr>
<td>Create rudimentary employee records that can be used by Oracle Fusion HCM, if you have it implemented or choose to implement it in the future.</td>
<td>Yes</td>
<td>Yes</td>
<td>You must specify each user either as an employee or as a contingent worker. When you create users, either one by one or through the data import, the application generates employee records for each user.</td>
</tr>
</tbody>
</table>

**Creating the Resource Reporting Hierarchy**

The resource reporting hierarchy, which you create by specifying managers when you create users, does not have to mirror the formal reporting hierarchy, which is captured separately in the Oracle Fusion HCM application, if it has been implemented.

---

**Note**

In Oracle Sales Cloud, you can have only one hierarchy reporting to one person.

You build a resource reporting hierarchy when you create sales application users by specifying the manager for each user. If you are creating users one-by-one in the user interface, then you must start by creating the user at the top of the
hierarchy and work your way down. If you are importing users using file-based import, then the order does not matter provided that all of your users are in the same file.

Creating Resource Organizations and the Resource Organization Hierarchy

In Oracle Sales Cloud, you must assign each manager that you create as a user with his or her own resource organization. All direct reports who are individual contributors inherit their manager's organization.

In Oracle Sales Cloud, resource organizations serve a limited purpose. Their names appear in the application's Resource Directory, which users can access to obtain information about their coworkers, and in social media interactions. Resource organizations are not used for work assignment. You assign work to individuals rather than their organizations.

The following screen capture shows the Resource Directory, which is available on the application Navigator. The resource organization names appear under each person's title.

The application automatically builds a resource organization hierarchy, using the resource reporting structure.

The resource organizations remain even if managers leave. You can reassign the resource organizations to their replacements.

The resource organization names do not have to reflect the names of departments. Departments are tracked along with employee records in the Oracle Fusion HCM application if it has been implemented. The resource organizations are not used in application security or to assign work to users. For example, you cannot include a resource organization on an opportunity sales team or as a territory owner.

Creating Basic Oracle Fusion HCM Employee Records

When you create application users, you must include information that is used to create basic employee records for the Oracle Fusion HCM application. This requirement is part of Oracle Sales Cloud architecture. These records are used only if you are implementing this application now or plan to do so.
The following table lists the information that you must enter in the Employment Information region of the Create User page, or in the import file.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Type</td>
<td>Enter either Employee or Contingent Worker, depending on whether the user you are creating is an employee or a contractor. The selection you make is used for provisioning either the Employee or the Contingent Worker abstract role.</td>
</tr>
<tr>
<td>Legal Employer</td>
<td>Enter the legal entity. Oracle creates the legal entity for you from the information you provide when you sign up for Oracle Sales Cloud.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Enter the business unit. Oracle creates the business unit for you from the information you provide when you sign up for Oracle Sales Cloud.</td>
</tr>
</tbody>
</table>

**About Provisioning Enterprise Roles to Users: Explained**

This topic describes how role provisioning is implemented in Oracle Sales Cloud.

**About Provisioning Enterprise Roles to Users**

You enable the provisioning of enterprise roles to users by creating provisioning rules using the Manage HCM Role Provisioning Rules task from the Setup and Maintenance work area. Each rule (also referred to as a mapping) includes one or more conditions, the list of enterprise roles you want to provision, and an option to make the provisioning automatic.

When you select automatic as an option, then the enterprise roles are provisioned automatically when you create the user if the user matches the rule conditions. It does not matter if you create users manually in the user interface, or import them from file.

When you are creating Oracle Sales Cloud application users, you provision job roles based on the role a user plays in the organization. This resource role merely provides the job title which appears in the company resource directory. The resource role should not be confused with the enterprise role, which provides the security permissions.

The following figure provides an example of how role provisioning rules work:

1. When you create sales manager user, you assign that user with the Sales Manager resource role. This is her title in the organization.
2. The role provisioning rule uses that resource role as a condition.
3. When you create a user with the sales manager resource role, then the condition is true and the rule automatically assigns the user with the Sales Manager job role and the Resource Abstract role.
Oracle provides you with resource roles that correspond to the job roles listed previously. Resource Role and Job Role names are the same except for the Salesperson resource role, which matches the Sales Representative job role.

**Steps for Setting Up Enterprise Role Provisioning**

You must set up role provisioning before you create users as follows:

- **Resource Roles.** If you are creating users with roles that are not provided by Oracle, or your organization uses different titles, create any additional resource roles that are required. Resource roles are used in provisioning roles to application users but not to setup users.

  For information on creating additional resource roles, see the topic Creating Resource Roles: Worked Example.

- **Employee Abstract Role.** Create a rule to provision the Employee abstract role to all users who are employees.

  This is a one-time setup. You create a separate rule to provision the Employee abstract role because this role is provisioned to application users and to users who are not sales resources, such as setup users.

  For information about creating the rule to provision the Employee abstract rule, see the topic Creating Setup Users for the Oracle Sales Cloud: Worked Example.

- **Job Roles.** Create the rules to provision users with the appropriate job roles. When you are creating the rule for application users, each rule must also provision the Resource abstract role. You can assign multiple enterprise roles to an individual.

  For information on creating provisioning rules for application users, see the topic Creating Rules to Automatically Provision Enterprise Roles for the Oracle Sales Cloud: Worked Example.
Creating Setup Users for Oracle Sales Cloud: Worked Example

This topic describes how to create setup users. The initial user you receive when you activate Oracle Sales Cloud can perform all of the application setup tasks. As a best practice, it is recommended that you create additional setup users with the type of broad setup privileges Oracle provides to the initial user you received.

**Note**

In Oracle Sales Cloud, setup users replace implementation users, described elsewhere in Oracle Applications documentation. Implementation users are set up in Oracle Identity Manager (OIM).

The setup users created in this example are not created as resources in your sales application. Because they are not resources, they do not appear in the sales organization directory and cannot be assigned work or be assigned to sales territories. However, you can provide the same setup permissions to users in the sales organization, if you need to.

Creating a setup user follows the same general procedure you use to create all users, with the following differences:

- You do not assign resource roles to setup users because you do not want them to be part of the sales organization.

- You must create a provisioning rule to assign users with the appropriate enterprise roles they require to do their job. When you create sales users, the provisioning rule is based on the resource role; when creating setup users, the provisioning rule must be based on another user attribute, such as a job.

To create the setup user in this example you do the following:

1. Create a job called Customer Administrator.
   
   You create this job for creating setup users only. The job does not serve any other purpose in Oracle Sales Cloud.

2. Create a provisioning rule that automatically provisions the following job roles to all users with the Customer Administrator job:
   
   - Application Diagnostics Administrator
   - Application Implementation Consultant
   - IT Security Manager

3. Create a separate provisioning rule that provisions every user of type employee with the Employee abstract role. All of your users are employees, so they all receive this role.

4. Create each setup user as a user of type employee with the Customer Administrator job.
Steps to Create the Job for Provisioning Setup Users

Use the following steps to create a job that you can use to assign setup users with the same implementation privileges as the initial user. You will use this job as a condition in the provisioning rule you create and add it to the user.

1. Sign in as the initial user or a user with implementation privileges, such as another setup user.
2. Open the Setup and Maintenance work area (Navigator - Tools - Setup and Maintenance).
3. On the Overview page of the Setup and Maintenance work area, search for the Manage Job task.
4. Click Go to Task.
   The Manage Jobs page appears.
5. Click Create.
   The Create Job: Basic Details page appears.
6. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Customer Administrator</td>
</tr>
<tr>
<td>Code</td>
<td>CustomerAdministrator. (No spaces)</td>
</tr>
</tbody>
</table>

You can keep the other values as they are because they are not used in Oracle Sales Cloud.
7. Click Next at the top of the page.
8. Click Submit on the next page, and dismiss the warning by clicking OK.
   You receive a notification when the job is created. This process can take a few minutes.

Steps to Create the Provisioning Rule for the Setup Job Roles

Use this procedure to create the provisioning rule that will automatically provision users assigned the Customer Administrator job with the same job roles as are provided by Oracle to the initial user.

1. Navigate to the Setup and Maintenance work area.
2. On the All Tasks tab, search for the Manage HCM Role Provisioning Rules task.
3. Click Go to Task.
   The Manage Role Mappings page appears.
4. Click Create.
   The Create Role Mapping page appears.
5. In the **Mapping Name** field, enter a name, for example, Setup User.

6. In the Conditions region, select the job you created earlier from the **Job** list. In this example, you select Customer Administrator.

7. If you have implemented Oracle HCM Cloud, then enter **Active** for **Assignment Status**.
   This additional condition ensures that the provisioned enterprise roles are automatically removed if the user is terminated.

8. In the Associated Roles region, click **Add** to add the following job roles:
   - Application Implementation Consultant
   - IT Security Manager
   - Application Diagnostics Administrator

9. Make sure the **Autoprovision** option is selected for each of the job roles.

10. Click **Save and Close**.

### Steps to Create the Provisioning Rule for the Employee Abstract Role

Use the following procedure to create a rule to provision the Employee abstract role to all users who are employees. This is a one-time setup. You can reuse the same rule for all employee users.

1. In the Manage Role Mapping page, click **Create** to create the second rule.
   The Create Role Mapping page appears.

2. In the **Mapping Name** field, enter a name, for example, Employee.

3. In the Conditions region, select **Employee** from the **Assignment Type** list.

4. If you have implemented Oracle HCM Cloud, enter **Active** for **Assignment Status**.
   This additional condition ensures that the provisioned enterprise roles are automatically removed if the user is terminated.

5. In the **Associated Roles** region, click **Add** to add the **Employee** enterprise role.

6. Make sure the **Autoprovision** option is selected for this role.

7. Click **Save and Close**.

### Steps to Create a Setup User

Use the following steps to create other setup users.

1. In the Navigator, select the **Manage Users** link under the **Manager Resources** heading.
   The Manage Users page appears.

2. Click **Create**.
   The Create User page appears.

3. Enter the user’s name and a unique e-mail address in the Personal Details region.
The application automatically sends the initial sign-in credentials to this e-mail address when you save the record.

You can leave the **Hire Date** as is. The Hire Date and the remaining fields are not used by Oracle Sales Cloud.

4. In the **User Details** region, enter the user name. If you leave the **User Name** field blank, then the application creates a user name based on the entries you have already made.

5. In the **User Notification** region, leave the **Send User Name and Password** option selected because you want the setup users to receive initial email notifications with their login and password details when you save the record.

6. In the **Employment Information** region, enter the information shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Type</td>
<td>Select Employee. The provisioning rule you set up is based on the employee’s job.</td>
</tr>
<tr>
<td>Legal Employer</td>
<td>Select the legal employer Oracle created for you using the information you provided when you signed up with Oracle Sales Cloud.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Select the business unit created for you using the information you provided when you signed up with Oracle Sales Cloud.</td>
</tr>
<tr>
<td>Job</td>
<td>Select Customer Administrator, the job you just created.</td>
</tr>
</tbody>
</table>

7. Click **Autoprov2isioning Roles**.

The Roles region displays the following roles:

- Application Diagnostics Administrator
- Application Implementation Consultant
- IT Security Manager
- Employee

8. Click **Save and Close**.

An email is sent to the new setup user containing the initial credentials for logging into the application.
Getting Ready to Create Application Users

What You Must Do Before Creating Application Users: Explained

Creating sales application users requires a bit more preparation than creating setup users. When you create sales application users, either in the UI or by importing them from a file, you not only provision the permissions the users need to do their jobs, but you also build the sales organization chart. This means that you must set up not only the provisioning rules, but also the elements that the application will use to create the organization chart, such as the root of the chart, and the job titles for each resource.

You are getting ready to create two types of application users:

- Members of the sales team without any system administration duties. These are the salespersons, the sales managers, and the sales vice presidents.
- At least one sales administrator user who will set up and administer the sales territories and sales processes.

Setup Overview

1. You must assign a title, called a resource role, to each sales user you create. The resource roles display right underneath user names in the resource directory and elsewhere in the UI.

You also use the resource roles as conditions in your provisioning rules. For example, you assign the Sales Manager job role to a user with the Sales Manager resource role.

Oracle provides standard resource roles, which correspond to the available job roles for sales, partner sales, and channel sales. For sales, these are:

- Sales Administrator
- Sales Manager
- Sales Vice President
- Salesperson
If you want other job titles to display for your users or if you want to provision some users with special privileges, then you must create additional resource roles using the Manage Resource Roles task from the Setup and Maintenance work area.

For example, you must create a CEO resource role if you want to include the CEO title in your organization chart. It's not one of the resource roles created for you.

You must also create additional resource roles, if you want to provide a small subset of resources with additional privileges. For example, if one of the sales managers in the organization is also in charge of maintaining territories and sales processes, you want to create a new resource role that you can provision with both the sales manager and the sales administrator job roles.

For details, see the topic Creating Additional Resource Roles.

2. Create a resource organization for the top manager in your hierarchy using the Manage Internal Resource Organizations task from the Setup and Maintenance work area.

You must assign resource organizations to all the manager users you create. All direct reports who are not managers inherit the organization. As you create users, the application creates an organization hierarchy that you can use to browse through the sales organization’s resource directory.

For details, see the topic Creating Resource Organizations.

**Note**

You can also create resource organizations while creating users in the Create User page.

3. Next, you must designate the resource organization you just created as the top of your organization tree, by using the Manage Resource Organization Hierarchies task in the Setup and Maintenance work area.

For details, see the topic Designating a Resource Organization as the Top of the Sales Hierarchy.

4. Decide what job roles you want to assign to your users.

Remember that you are not restricted to assigning one job role to a user. For example, you will want to provision the sales manager in charge of determining sales territories and sales processes with the Sales Administrator job role in addition to the Sales Manager job role. This will enable this resource to perform the required sales setups.

You must create at least one user with the Sales Administrator job role to perform these setups.

5. Using the Manage HCM Role Provisioning Rules task, set up the provisioning rules to automatically provision the appropriate job roles.
Getting Ready to Create Application Users

and the Resource abstract role to your users based on their resource role. You must create a provisioning rule for every resource role. For details, see the topic Creating Rules to Automatically Provision Enterprise Roles to Sales Users.

6. When you create users, the application automatically sends e-mails with the sign-in credentials to the users. You can configure this behavior as described in the topic Setting Up E-Mail Notifications for New Users: Procedure.

Creating Resource Organizations

Use this procedure to create resource organizations for managers in your sales organization. You must create a resource organization for every manager, including the top manager, usually the CEO. You must use this procedure for the top manager and for any other managers you create in the UI. When you import users from a file, you can create the resource organizations automatically from the information you include in the file itself.

Creating a Resource Organization

1. Search for the Manage Internal Resource Organizations task in the Setup and Maintenance work area.

2. Click Go to Task.
   The Manage Internal Resource Organizations page appears.

3. Click Create.
   The Create Organization: Select Creation Method page appears.

4. Select Option 2: Create New Organization.

5. Click Next.

6. Enter the name of the resource organization in the Name field. This is the name that will be visible in the resource directory.
   • Each resource organization name you enter must be unique.
The names do not have to correspond to any formal organization in your enterprise. They are there solely to create a resource directory. Do not use managers’ names, as you may want to reassign the organizations to others later.

7. In the Organization Usages region, click Add Row and select Sales Organization.

8. Click Finish.

Designating a Resource Organization as the Top of the Sales Hierarchy

After you have created the resource organization for the top person in the sales organization, you are ready to designate that resource organization as the top of the sales hierarchy.

Designating the Organization You Created as the Top of the Sales Hierarchy

1. Search for the Manage Resource Organization Hierarchies task in the Setup and Maintenance work area.

2. Click Go to Task.
   The Manage Resource Organization Hierarchies page appears.

3. Click Search.

4. In the search results, select the Internal Resource Organization Hierarchy link. This value is supplied by Oracle.

5. From the Action menu at the top right-hand corner of the page, select Edit This Hierarchy Version.
   The View Organization Hierarchy page appears.

   The Edit Organization Hierarchy Version page appears.
6. Click **Add** in the Internal Resource Organization Hierarchy region.

   ![](image1)

   The Add Tree Node window appears.

7. Click **Search**.

   ![](image2)

   The Search Node window appears.

8. Click **Search** again in the Search Node window.

9. Select the resource organization that you created in the Creating a Resource Organization procedure.
10. Click **OK**.

   The application returns you to the Edit Organization Hierarchy Version page.

11. Click **Save and Close**.

12. When a warning appears, click **Yes**.

## Creating Additional Resource Roles

Follow the steps in this topic to create additional resource roles.

After you create a resource role, you must create the appropriate provisioning rules to provision the user with the required enterprise roles. The resource role by itself is only a title.

### Creating a Resource Role

1. Navigate to the Setup and Maintenance work area using the Navigator menu.

2. Search for the Manage Resource Roles task.

3. Click **Go to Task**.

   The Manage Resource Roles page appears.

4. Click **Create**.

   The Create Role page appears.
5. In the Role Name field, enter the name of the resource role as it will appear in the application UI, for example, CEO.

6. In the Role Code field, enter a unique internal name. No spaces are permitted. If you are importing users from a file, then you must include this code in your file rather than the name.

7. Select the Manager option, if the resource role belongs to a manager, or the Member option, if the resource role belongs to an individual contributor.

8. From the Role Type list, select Sales to classify the role that you are creating.

9. Click Save and Close.

Creating Rules to Automatically Provision Enterprise Roles to Sales Users

You must create rules to automatically provision Oracle Sales Cloud application users with the necessary enterprise roles to perform their jobs before you create users. The provisioning is based on the resource role that you assign to a user, so you must create a rule for every resource role you use in your organization. You must create rules to provision all of the resource roles provided by Oracle as well as all the additional resource roles you created, such as the CEO.

Creating a Provisioning Rule

1. Sign in as a setup user.

2. Navigate to the Setup and Maintenance work area and search for the Manage HCM Role Provisioning Rules task.

3. Click Go to Task.

The Manage Role Mappings page appears.
4. Click **Create**.

The Create Role Mapping page appears.

5. In the **Mapping Name** field, enter a name that will help you identify the mapping, for example, *Sales Vice President*.

6. In the Conditions region, select the resource role you want to provision from the **Resource Role** list. For example, *Sales Vice President*.

7. If you have implemented Oracle Global Human Resources Cloud Service, then enter **Active** for **Assignment Status**.

   This additional condition ensures that the provisioned enterprise roles are automatically removed if the user is terminated in Global Human Resources.

8. In the Associated Roles region, click **Add** to add the enterprise roles you want to provision. For the sales vice president, you add the following:

   - **Sales Vice President**
   - **Resource**

   **Note**

   Each sales resource must be provisioned with both the Resource and Employee abstract roles. You already created a rule to provision the Employee abstract role when you created setup users.

9. Make sure the **Autoprovision** option is selected for all the enterprise roles.

10. Click **Save and Close**.

### Setting Up E-Mail Notifications for New Users: Procedure

This topic describes how to configure the credential e-mails sent to new users.
For each Sales user that you create, you must enter a unique e-mail address. By default, the application automatically sends an e-mail notification with the user name and temporary password assigned to the user to this address immediately after the user is created. When users sign in with their temporary passwords, they must change their passwords and enter the security challenge questions. These questions cannot be edited later, although they can be reset by logging a service request on support.oracle.com.

You can configure how and when credential emails are sent as follows:

- You can choose to redirect the initial credentials e-mail sent to users to a single user. For example, you might want to send all of the credential e-mails to one of the setup users when testing your implementation.

- After you have tested your implementation and are starting to create Sales users, you can choose to send the credentials emails to new users in bulk, rather than sending individual notifications as each user is created.

The following procedures describe each of these tasks.

**Designating a Single User to Receive All Credential E-Mails**

You can set up a small number of test users, so that you can test your implementation from the point of view of different user roles such as a salesperson, a manager, and a sales administrator. You can later inactivate these users, so they are not visible in the application.

When you set up test users, have the initial password notifications sent to one of the setup users using the steps below:

1. Navigate to the **Setup and Maintenance** work area.
2. Search for the task **Manage Enterprise HCM Information** on the All Tasks tab of the Overview page.
3. Click the **Go to Task** button.
4. In the Enterprise page, click the **Edit** button, then select **Correct**.
   - The Edit Enterprise page is displayed.
5. In the User and Role Provisioning Information region, in the **Alternate Contact E-Mail Address** field, enter the e-mail address of the user who you want to receive the initial credentials e-mails.
6. Make sure the **Send User Name and Password** option is set to **Yes**.
7. Click **Submit**.
8. Click **Done**.

When you start to create Sales users, remove the e-mail address from the **Alternate Contact E-Mail Address** field so that the e-mails are again sent to new users rather than a setup user or administrator.

**Note**

The application sends the e-mails with initial passwords only once, so, if you choose to send the initial e-mail to a setup user, you will have to resend the credentials to the real user yourself.
Sending E-Mail Notifications to All Users in Bulk

The following procedure describes how to send credential email notifications to all new users at the same time, instead of when each individual user is created.

1. On the Edit Enterprise page, User and Role Provisioning Information region, set the Send User Name and Password option to No so that credentials emails are not sent to individual new users.
2. In the Navigator, select Scheduled Processes under the Tools heading.
4. In the Schedule New Process dialog box, make sure the Job option is selected for Type.
5. Select Send User Name and Password E-Mail Notifications in the Name field.
6. Click OK.
7. In the Process Details window, click Submit.
8. Click Close.

Note
The Send User Name and Password E-Mail Notifications process sends the notification e-mail only to those users who have never been sent the notification. The process does not reset passwords or resend the notification.
Creating Application Users

Creating Application Users for Oracle Sales Cloud: Worked Example

Follow the steps in this example to create Oracle Sales Cloud application users. Before creating application users, make sure you have:

- Set up any additional resource roles and autoprovisioning rules for enterprise roles.
- Created the resource organizations that you will assign to each manager. You can also create the resource organization while creating each manager user.

When you create application users, you automatically set up the reporting hierarchy of your organization by indicating each person's manager. For this reason, you must first create the user at the top of the hierarchy and work your way down.

**Steps to Create an Application User**

To create an application user:

1. In the Navigator, select the Manage Users link under the Manager Resources heading.
   
   The Manage Users page appears.

2. Click Create.
   
   The Create User page appears.

3. In the Personal Details region, enter the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Enter the user's last name. This entry is required.</td>
</tr>
<tr>
<td>First Name</td>
<td>Optionally, enter the user's first name.</td>
</tr>
</tbody>
</table>
4. In the User Details region, enter the user name. If you leave the User Name field blank, the application creates a user name using the entries you already made.

You can leave the Hire Date as is. The Hire Date and remaining fields are not used by Oracle Sales Cloud. They are important only if you implement Oracle HCM.

5. In the User Notification region, you can select the Send User Name and Password option if you want to send the e-mail notification with the login and password to the user when you save the record.

6. In the Employment Information region, enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Type</td>
<td>Select Employee.</td>
</tr>
<tr>
<td>Legal Employer</td>
<td>Select the legal employer Oracle created using the information you provided when you signed up with the service.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Select the business unit Oracle created using the information you provided when you signed up with the service.</td>
</tr>
</tbody>
</table>

7. In the Resource Information region, enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Role</td>
<td>Select the role the user plays in the resource organization.</td>
</tr>
<tr>
<td>Reporting Manager</td>
<td>Select the user’s manager.</td>
</tr>
<tr>
<td></td>
<td>If you are creating the top user in your hierarchy, such as the CEO, you can leave this field blank.</td>
</tr>
</tbody>
</table>
### Enabling Single Sign-On for Your Applications: Explained

You can make it possible for your users to use a single user name and password to sign in to all of your on-premises and Oracle Sales Cloud applications by implementing Oracle Enterprise Single Sign-On.

Oracle Enterprise Single Sign-On (SSO) is available for customers who have implemented either the Microsoft Active Directory Federation Server (AD FS) 2.0 or the Oracle Identity Federation Service 11g identity provider (IdP). Other identity providers require special approval. Here is the standard approval process:

1. You contact your salesperson or open a service request for SSO Enablement on support.oracle.com.
2. Your Oracle sales or support representative sends you a questionnaire to fill out.
3. After you return the questionnaire, Oracle representatives evaluate your responses and obtain approval, usually within 24 hours.
4. After you are approved, Oracle sets up your Oracle Sales Cloud environment and you receive the appropriate documentation on setting up your system.

It typically takes a minimum of two weeks or more for Oracle to implement the SSO for your Oracle Sales Cloud environment after you obtain necessary approval.
Managing Application Users

Resetting User Passwords: Procedure

This topic describes how to update a user account by changing the user's password.

When new users are created in Oracle applications, they receive a login and a temporary password which they can change. If necessary, you can reset a user's password at any time by performing the steps in the following procedure.

1. In the Setup and Maintenance work area, select the All Tasks tab of the Overview page.
2. Search for the task Manage Job Roles.
3. Click Go to Task.

The Oracle Identity Manager Self-Service page opens.
4. Click the Administration link in the top-right corner of the page.

The Oracle Identity Manager - Delegated Administration page opens.
5. In the Search area, search for the user whose password you want to change, then select the user from the search results.
6. In the new tab that opens for the user, click Reset Password.

In the Reset Password dialog box, choose one of the following options, then click Reset Password:

- **Manually Change the Password.** If you select this option, you must enter the new password for the user. You can also choose whether or not the new password is sent to the user's primary work email.

- **Auto-generate the Password (Randomly generated).** If you select this option, a temporary password is generated and sent to the user's primary work email.
Changing User Resource Roles When Job Assignments Change: Procedure

If an employee takes on a different role within the company, for example, if the user is promoted, then you must update the resource role assigned to the employee as described in this topic.

Changing the resource role assigned to an employee involves:

- Assigning a new resource role to the user that corresponds to the new assignment, for example, Sales Manager
- Setting an end date for the old resource role, for example, Salesperson

Perform the steps in the following procedure to change a user’s resource role.

1. In the Setup and Maintenance work area, select the All Tasks tab on the Overview page.
2. Search for and select the task Manage Resources.
3. On the Manage Resources page, search for and select the resource. The Resource page for the individual opens.
4. Click the Roles tab, then click Add and add the new resource role for the user, for example, Sales Manager.
5. In the Roles list, select the current role assigned to the user, for example, Salesperson, and enter an end date in the To Date field. The value you enter is the date the user’s assignment in the current role ends.
6. Click Save and Close.
7. To automatically provision any roles that you have set up using the role provisioning rule for the new resource role you just assigned the user, do the following:
   - On the All Tasks tab on the Overview page, search for and select the task Manage Users.
   - On the Manage Users page, search for and select the relevant user.
   - On the Edit User page for the user, click the Autoprovision Roles button in the Resource Information section.
     In the Current Roles section, you can remove any individual role if it is on longer required.

Terminating User Accounts: Procedure

This topic describes how to terminate user accounts if an employee leaves your company.
You cannot delete a user account. However, when an employee leaves your company, you can suspend the user account by completing both of the following steps:

1. Perform either one of the following tasks:
   - Inactivate the user’s account
   - Remove the user’s roles
2. Set an end date for the resource

**Note**

The process outlined in this topic applies if you are using Oracle Sales Cloud only. If your company uses Oracle HCM Cloud along with Oracle Sales, then a different process applies.

### Inactivating a User Account

When an employee leaves your company, in most cases it is recommended that you inactivate the user account. Inactivating the user’s account prevents the user from being able to log in to the application.

To inactivate a user account, perform the steps in the following procedure.

1. In the Setup and Maintenance work area, select the All Tasks tab of the Overview page.
2. Search for and select the task Manage Users.
   
   The Manage Users page opens.
3. Search for and select the user whose account you want to inactivate. The Edit User page for the user opens.
4. In the User Details section, in the **User Account Status** field, select **Inactive**.
5. Click **Save and Close**.

### Removing Roles From a User

Instead of inactivating the user account, you can remove some or all of the roles assigned to the user. You might want to do this if you want to keep some roles active. For example, maybe you want to keep the user account valid to allow the user access to your custom pages.

To selectively remove roles from a user, perform the steps in the following procedure.

1. Navigate to the Manage Users page as described in the previous task.
2. Search for and select the user whose roles you want to remove.
   
   The Edit User page for the user opens.
3. In the Current Roles section, select the role you want to remove, then click the **Remove** button. Repeat this process for each role assigned to the user that you want to remove.
4. Click **Save and Close**.

**Setting an End Date for the Resource**

After you have either inactivated a user account or removed the roles assigned to a user account, you must set an end date for the resource (user) as described in this topic.

To set the end date for a user, perform the steps in the following procedure.

1. In the Setup and Maintenance work area, select the All Tasks tab of the Overview page.
2. Search for and select the task Manage Resources.
   
   The Manage Resources page opens.
3. Search for and select the resource you want to edit. The Resource page for the individual opens.
4. In the **To Date** field, enter the date the individual is leaving the company.
5. Click **Save and Close**.

**Note**

You can also set the end date for an employee in the Resource Directory which you can access from the Navigator menu.

Upon the end date you specify for a resource, the following occurs:

- The terminated employee is no longer available in the application so can no longer be newly associated with any Sales objects, such as sales account, territory, lead, and opportunity. The user's association with Sales objects made before the end date are not automatically removed but you can remove them manually.
- Resource roles for the individual are deprovisioned.

**FAQs for Terminating Users**

**How are the records of a terminated employee reassigned?**

After you terminate an employee in the application, the assignment process automatically excludes the terminated employee when it runs again. However, you have to manually handle other reassignments, for example, you must manually replace the terminated employee with another employee on the territory team or sales account team.

**Can I reactivate a terminated employee record?**

Once you have specified an end date for a resource, it cannot be reversed in Oracle Sales. However, the ex-employee's record remains in the system so you
can re-identify that person as a resource if the person is rehired. After that, you will need to do role and organization assignment again.
Customizing Security

Security Customization: Overview

This chapter describes some of the ways in which you can customize the Oracle Sales Cloud security model.

The Oracle implementation of role-based access control (RBAC) is designed to handle a wide range of security requirements in different environments. As a result, most companies can use the standard security settings without modification. If necessary, however, you can configure the default settings to meet specific business requirements. For example, you can add or remove duty roles from a job role to extend or limit the data or functionality provided by the job role.

This chapter describes how to:

• Create new job roles and associate them with existing duty roles
• Create custom duty roles and assign functional privileges and data security policies to them
• Remove users ability to create accounts
• Restrict access to sales accounts

Note
In general, you make changes to the standard security settings using Authorization Policy Manager. Most changes take immediate effect and can be viewed after you return to the Authorization Management Home page. Changes to role hierarchy behavior can, however, take up to 20 minutes to take effect.

Recommendations for Customizing Security

This topic provides some recommendations for customizing the security reference implementation.

For additional information about changing the standard security settings for specific releases of Oracle Sales Cloud, go to the Security Resource Center, which is available at 1609084.1 (Article ID) on My Oracle Support. The Security Resource Center provides detailed instructions for performing security configuration tasks, and provides templates you can use to track the changes you make to standard settings.
General Recommendations

Review the following recommendations before customizing the default security settings.

- Use the default security settings whenever possible but, if customizations are required, review the proposed changes with Oracle Support.
- Clearly define the change that is required.
- Make sure you understand the interrelationships of the various security components and the effect of the proposed change on user access.
- Document any changes you make.
- Create custom roles rather than modifying predefined roles.

Upgrade Considerations

If you change the security reference implementation, then conflicts can occur when upgrades and maintenance patches are applied to the application. The Oracle Sales Cloud operations team will report any conflicts that occur, and you can choose to accept or reject the changes that caused the conflicts.

You can either:
- Reject the change. The customization you made is overwritten.
- Accept the change. The customization you made is preserved.

Creating a Custom Job or Abstract Role: Procedure

If the predefined job or abstract roles don’t meet enterprise requirements, then you can create new job or abstract roles. For example, you might want to create a new job role because the duties inherited by a predefined job role aren’t as required. This topic describes how to create a job role. This procedure has two stages:

1. Create the job role in Oracle Identity Manager (OIM) using the Manage Job Roles task.
2. Add duty roles to the new job role in Authorization Policy Manager using the Manage Duties task.

In Authorization Policy Manager, duty roles are known as application roles.

Creating the Job Role

Sign in to Oracle Sales Cloud with the IT Security Manager job role and follow these steps.

1. Navigate to the Setup and Maintenance work area.
2. On the All Tasks tab of the Overview page, search for and select the task Manage Job Roles.
3. In the search results list, click the Go to Task icon. The Oracle Identity Manager Self-Service page opens.
4. On the Welcome tab of the Oracle Identity Manager Self-Service page, click the Administration link in the top-right corner. The Oracle Identity Manager - Delegated Administration page opens.

5. In the Roles section of the Welcome tab, click Create Role. The Create Role page opens.

6. In the Name field, enter the name of the new role, for example, INSIDE_SALES_REP_JOB.

7. In the Display Name field, enter the display name of the job, for example, Inside Sales Representative.

8. In the Role Category Name field, search for and select CRM - Job Roles.

9. Click Save. The job role is now created in the LDAP identity store.

Close the OIM browser window to return to the Oracle Fusion Applications Setup and Maintenance work area.

Assigning Duties to the Job Role

Follow these steps to assign one or more duties to the new job role.

1. Navigate to the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

3. In the search results list, click the Go to Task icon. The Oracle Entitlements Server page opens.

4. In the Application Name section of the Authorization Management page, select crm.

5. In the Search section, search for the new job role you created. A job role is an external role with a global scope, so specify the following search criteria:
   - For External Roles
   - In Global Scope
   - In the search text box, enter the name of the job role you created, for example, Inside Sales Representative.

6. In the search results area, select the role and click View.

7. On the role page, click the Application Role Mapping tab.

8. Click Map.

The Map Application Roles to External Role dialog box opens.

   - In the Application field in the Map Application Roles to External Roles dialog box, select crm.
   - In the Display Name field, enter the name of the duty role that you want to add, for example, Sales Representative Duty, and click Search.
   - Select the role in the Search Results, and click Map Roles.

Tip
The selected role appears under the crm folder on the Application Role Mapping tab of the role page. You can also delete duty roles on this tab.

9. Repeat Step 8 for additional duty roles.

Close the Authorization Management browser window to return to the Oracle Fusion Applications Setup and Maintenance work area.

Creating Custom Duty Roles: Procedure

Duty roles are made up of functional security privileges and data security policies. You can create custom duty roles if the predefined duty roles don't meet your needs. For example, a predefined duty role might have more functional security privileges or data security policies than are required. This topic shows how to:

- Create a duty role.
- Select existing functional security privileges and add them to a duty role.
- Select existing data security policies and add them to a duty role.

Creating a Duty Role

Sign in to Oracle Sales Cloud with the IT Security Manager job role and follow these steps:

1. Navigate to the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the task Manage Duties.

3. In the Search Results list, click Go to Task.

   The Authorization Management page opens.

4. In the Application Name section of the Home tab, select crm. Under the Application Roles heading on the Home tab, click New.

   An Untitled tab opens.

5. In the Display Name field on the Untitled tab, enter the display name of the new duty role, for example, Custom Sales Representative Duty. In the Role Name field, enter the name of the new duty role, for example, Custom_Sales_Rep_Duty.

6. Click Save.

   The duty role’s display name now appears as the tab name.

Adding Functional Security Privileges to a Duty Role

In this stage, you create a security policy for the custom duty role you created, and add an existing functional security privilege to it.

1. Click Create Policy in the top-right corner of the duty role tab, then select Default Policy Domain.

   An Untitled tab opens.
2. In the **Display Name** field on the Untitled tab, enter the policy name, for example, *Policy for Custom Sales Representative Duty*.

---

**Tip**

Names of predefined security policies begin with the words *Policy for*.

---

3. In the **Name** field, enter the policy name, for example, *CUSTOM_SALES_REP_DUTY_POL*.

4. In the Targets section, click **Add Targets**.
   
   The Search Targets dialog box opens.

---

**Tip**

In this context, a target is a functional security privilege and a principal is a role. When a target is granted to the principal, it means that the functional security privilege is granted to the duty role.

---

5. In the **Display Name (Starts With)** field on the Entitlements tab, enter the name of the functional security privilege that you want to use, for example, *Manage Opportunity Sources*, and click **Search**.
   
   In the search results, select the functional security privilege and click **Add Selected**. The functional security privilege is added to the Selected Targets section.

6. Click **Add Targets** to close the dialog box.

7. On the Untitled tab, click **Save**. The Untitled tab is updated with the name of the new policy, for example, *Policy for Custom Sales Representative Duty*.

---

### Adding Data Security Policies to the Duty Role

In this stage, you’ll find the data security policies assigned to an existing duty role and add them to the custom duty role you created.

1. Click the Authorization Management Home tab. On the Home tab, click **Search** under the Application Roles heading. The Role Catalog page opens.

2. In the **Display Name** field in the Search Roles section, enter the name of the predefined duty role to be used as a reference for your custom duty role. For example, enter *Opportunity Sales Representative Duty* and click **Search**. Select the role in the Search Results and click **Open**.
   
   The *Opportunity Sales Representative Duty* page opens.

3. In the top-right corner of the page, click **Find Policies**, then select **Default Policy Domain**. The Search Authorization Policies tab opens.

4. In the Policies for: *Opportunity Sales Representative Duty* section, select the Data Security tab.
   
   The data security policies for the duty role appear on the tab.

5. Select the first data security policy that you want to use and click **Edit**.

   Search for your new duty role. For example, enter Custom_Sales_Rep_Duty in the Role Name field, select crm as the Application, and click Search.

7. Select the new duty role, for example, Custom Sales Representative Duty, and click OK.

   A copy of this data security policy now exists against your custom duty role.

8. Click Save. Click OK to close the confirmation window.

9. Repeat steps 5 through 8 to add additional data security policies to your duty role.

Your custom duty role is now complete.

Verifying the Duty Role

In this stage, verify that the custom duty role you created is assigned the functional security privileges and data security policies you mapped to the role.

1. Click the Authorization Management Home tab.

2. On the Home tab, select crm in the Application Name field and select Search under Application Roles. The Role Catalog page opens.

3. Search for the custom duty role you created, for example, Custom Sales Representative Duty.

   In the search results, select the duty role and click Open. The duty role page opens.

4. Click Find Policies, then select Default Policy Domain.

   In the Policies for: Custom Sales Representative Duty section, click the Functional Policies tab and then the Data Security tab to view the functional security privileges and data security policies you associated with the role.

5. Click the Home tab.

You can now assign the custom duty role you created to a job role.

Removing Create Account Functionality: Procedure

This topic describes how to disable the account creation functionality in Oracle Sales Cloud. You might want to remove the ability to create accounts if, for example, your organization's customers are individual consumers, not businesses, or if you use an external application to create accounts. Removing the functionality to create accounts involves two stages:

1. Delete the Create Sales Organization functional privilege from the following duty roles:
   
   • Sales Party Management Duty
• Marketing Sales Party Management Duty
• Partner Sales Party Management Duty

2. Delete the following resources from privileges in Authorization Policy Manager:

• ZcmCustomerPopupTF.xml
• ZcmCreateCustRegionalTF.xml
• ZcrmFuseCreateCustomerTF.xml

---

**Note**

In Authorization Policy Manager, privileges are known as entitlements.

---

After performing the steps in this procedure, links and buttons to create accounts are removed or disabled in the user interface.

**Delete the Create Sales Organization Privilege from Duty Roles**

Perform the steps in the following procedure to delete the Create Sales Organization functional privilege from duty roles.

1. Navigate to the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task, then in the search results list, click the Go to Task icon.

   The Authorization Policy Manager page opens.

3. In the Search area, specify the following search criteria:

   • For Application Roles
   • In crm
   • In the search text box, enter SALES PARTY MANAGEMENT DUTY

4. In the Search Results list, select the duty and click Open.

5. On the SALES PARTY MANAGEMENT DUTY page, click Find Policies in the top right corner of the page, then select Default Policy Domain.

6. In the Found Principles list, make sure that ZMC_SALES_PARTY_MANAGEMENT_DUTY is selected.

7. In the Policies for: section, click the Functional Policies tab.

8. From the Actions menu, click Open to display all the privileges associated with the policy.

9. In the Targets list, navigate to the Create Sales Organization privilege.

10. Select the privilege and click the Remove Target icon.

Delete Resources from Entitlements

Remove resources that expose the create account functionality from any entitlements that contain them by performing the steps in the following procedure.

1. Navigate to the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

3. In the search results list, click Go to Task. The Authorization Policy Manager page opens.

4. In the Application Name section of the Home tab, select crm.

5. Under the Entitlements heading on the Home tab, click Search. The Search Entitlements tab opens.

6. To remove the ZcmCustomerPopupTF.xml resource from entitlements, perform the following steps:
   • In the resource Name field, select Contains, then enter ZcmCustomerPopupTF.xml in the text field. Click Search. All entitlements that contain the ZcmCustomerPopupTF.xml resource are displayed in the Search Results list.
   • Highlight the first entitlement where you want to remove the popup, then click Open. All the resources associated with the entitlement are displayed.
   • Sort the information by Name, and expand the columns so that you can see the entire names.
   • Scroll down the list and highlight the row for the resource ZcmCustomerPopupTF.xml (/WEB-INF/oracle/apps/customerCenter/application360/publicUi/flow/ZcmCustomerPopupTF.xml#ZcmCustomerPopupTF ).
   • Click the Remove icon, then click Apply.
   • Click the Search Entitlements tab to return to the Search Results list and repeat the process for each of the other entitlements that contains the ZcmCustomerPopupTF.xml resource.

7. To remove the ZcmCreateCustRegionalTF.xml resource from any entitlements that contain it, repeat the procedure in step 4 with the following differences:
   • In the Search Entitlements page, search for ZcmCreateCustRegionalTF.xml
   • In each entitlement, delete the resource CreateCustRegionalTF.xml (/WEB-INF/oracle/apps/customerCenter/application360/publicUi/flow/ZcmCreateCustRegionalTF.xml#ZcmCreateCustRegionalTF).

8. To remove the ZcmFuseCreateCustomerTF.xml resource from any entitlements that contain it, repeat the procedure in step 4 with the following differences:
• In the Search Entitlements page, search for ZcmFuseCreateCustomerTF.xml
• In each entitlement, delete the resource ZcmFuseCreateCustomerTF.xml (/WEB-INF/oracle/apps/customerCenter/application360/publicUi/flow/ZcmFuseCreateCustomerTF.xml # ZcmFuseCreateCustomerTF.xml)

9. You might have to stop and restart the Oracle Authorization Policy Manager server for the changes to take effect.

Restricting Access to Sales Accounts: Worked Example

By default, the Sales Representative job role permits salespersons to access all accounts in the enterprise. This topic shows you how to restrict their access by customizing a duty role in that job role.

With the customized job role, users with this job role can only gain access to accounts when they meet one of the following criteria. They must be:

• in the sales account team
• in the sales account team with edit access
• in the sales account team with full access
• in the management chain of a resource who is on the sales account team
• in the management chain of a resource who is on the sales account team with edit access
• in the management chain of a resource who is on the sales account team with full access
• the owner of the territory associated with the sales account
• the owner of the territory that is an ancestor of the territory associated with the sales account
• a member of the territory associated with the sales account
• a member of the territory that is an ancestor of the territory associated with the sales account

All users with the Sales Representative job role retain access to all prospects in the enterprise.

Investigation

An investigation of the Sales Representative job role hierarchy reveals that the data security policies that control the unrestricted access to Sales Accounts are as listed below.

<table>
<thead>
<tr>
<th>Role</th>
<th>Actions</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Organization,</td>
<td>All Values</td>
</tr>
<tr>
<td>(FSCM)</td>
<td>Read</td>
<td></td>
</tr>
<tr>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>(FSCM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Organization,</td>
<td>All Values</td>
</tr>
<tr>
<td>(HCM)</td>
<td>Read</td>
<td></td>
</tr>
</tbody>
</table>
Notice that some of these policies are used by other application groups like FSCM and HCM. When a user with the Sales Representative role logs into the Oracle Sales Cloud application, these policies are evaluated by the security framework as and when the user navigates to sections of the application that are controlled by those policies. Eventually, all policies are evaluated and the most permissive access is granted to the Sales Representative. In this case all the above policies grant full access to Sales Accounts as indicated by the values in the condition column. Note that Sales Accounts can be Organizations, Contacts or Groups.

**Plan of Action**

For a Sales Representative, we want to replace the above duty roles where possible or change policies where needed. But we want to make sure that other roles are not adversely affected.

Each of the above policies control access to the database resource called Trading Community Person that is based on the HZ_PARTIES table. In Oracle Sales Cloud, the transactional data that appears in the Customer Center are instances of the Account entity and are stored in the HZ_PARTIES table. The Trading Community Person database resource is the base object for Sales Accounts, Contacts, and Prospects as well as other critical enterprise entities like Users and internal Organizations.

For the Sales Representative, we need a condition or rule that can be applied to the Trading Community Person object which will separate the critical enterprise entities from transactional Sales Account data. We can then use this condition to build custom policies for the Sales Representative. A further investigation of the Sales Representative hierarchy reveals that there is a data security policy already provided that can limit access to Sales Accounts and Prospects, as shown below. We can reuse this condition to build custom duty roles and policies for the Sales Representative to replace the duty roles and policies mentioned in the previous section.

<table>
<thead>
<tr>
<th>Role</th>
<th>Actions</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Party Information Inquiry Duty (HCM)</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Organization, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Sales Party Review Duty</td>
<td>View Sales Party, Read</td>
<td>Access the sales party for table HZ_PARTIES for all sales accounts in the enterprise</td>
</tr>
</tbody>
</table>

Notice that some of these policies are used by other application groups like FSCM and HCM. When a user with the Sales Representative role logs into the Oracle Sales Cloud application, these policies are evaluated by the security framework as and when the user navigates to sections of the application that are controlled by those policies. Eventually, all policies are evaluated and the most permissive access is granted to the Sales Representative. In this case all the above policies grant full access to Sales Accounts as indicated by the values in the condition column. Note that Sales Accounts can be Organizations, Contacts or Groups.
Once we have the new duty roles and the new policies, we can replace the duty roles that grant full access to the Sales Representative. A summary of custom-tailoring is listed below, indicating what we should do with the standard policies.

<table>
<thead>
<tr>
<th>To Do</th>
<th>Role</th>
<th>Actions</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New Policy</td>
<td>Party Information Inquiry Duty (FSCM)</td>
<td>View Trading Community Organization, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Create New Policy</td>
<td>Party Information Inquiry Duty (FSCM)</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Create New Policy</td>
<td>Party Information Inquiry Duty (HCM)</td>
<td>View Trading Community Organization, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Create New Policy</td>
<td>Party Information Inquiry Duty (HCM)</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Change Policy Condition</td>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Organization, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Delete Policy</td>
<td>Party Information Inquiry Duty</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Delete Policy</td>
<td>Sales Party Review Duty</td>
<td>View Sales Party, Read</td>
<td>Access the sales party for table HZ_PARTIES for all sales accounts in the enterprise.</td>
</tr>
</tbody>
</table>

**Customizing Security for the Sales Representative Role by Creating Duty Roles**

1. Login to Oracle Sales Cloud using your administrator credentials and navigate to the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Data Security Policies task.

3. In the search results list, click **Go to Task**.

   The APM home page opens.

4. Create a new duty role to replace Party Information Inquiry Duty (FSCM) duty role:
   - In the Home page, select FSCM in the Application Name list.
   - In the Application Roles section, click the **New** action link. The new role tab appears.
• Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>New Party Information Inquiry Duty (FSCM)</td>
</tr>
<tr>
<td>Role Name</td>
<td>NEW_PARTY_INFORMATION_INQUIRY_DUTY_FSCM</td>
</tr>
<tr>
<td>Description</td>
<td>Views trading community parties other than sales accounts and sales prospects.</td>
</tr>
</tbody>
</table>

• Click Save. The new role appears.

5. Create the first data security policy for the new duty role:

• From the top right corner of the role tab, click Find Policies.

• Click Default Policy Domain. The Search Authorization Policies tab appears.

• Check that the role name appears in the Found Principals list.

• At the bottom section, select the Data Security tab.

• In the Data Security tab toolbar, click the New icon. The New Policy tab appears with all fields blank.

• Enter the values shown in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Grant on Trading Community Organization</td>
</tr>
<tr>
<td>DB Resource</td>
<td>Trading Community Person (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
<tr>
<td>Module</td>
<td>Trading Community Model (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
<tr>
<td>Start Date</td>
<td>Use the calendar icon to select yesterday’s date.</td>
</tr>
</tbody>
</table>
• Click the Roles tab. Check the role name is NEW_PARTY_INFORMATION_INQUIRY_DUTY_FSCM.

• Click the Rule tab. Enter the values shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Set</td>
<td>Multiple Values</td>
</tr>
<tr>
<td>Condition</td>
<td>Access the trading community person for table HZ_PARTIES for all people in the enterprise other than sales accounts and sales prospects. (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
</tbody>
</table>

• Click the Action tab and move the values View Trading Community Organization and Read from the Available Actions list to the Selected Actions list.

• Click Save. The confirmation dialog appears. Click OK.

6. Create the second data security policy for the new duty role.

• In the Data Security tab toolbar, click the New icon. The New Policy tab appears with all fields blank.

• Enter the values shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Grant on Trading Community Person.</td>
</tr>
<tr>
<td>DB Resource</td>
<td>Trading Community Person (IMPORTANT: Do not enter directly. Use Search and select)</td>
</tr>
<tr>
<td>Module</td>
<td>Trading Community Model (IMPORTANT: Do not enter directly. Use Search and select).</td>
</tr>
<tr>
<td>Start Date</td>
<td>Enter yesterday's date (use the calendar icon).</td>
</tr>
</tbody>
</table>

• Click the Role tab. Check the role name is NEW_PARTY_INFORMATION_INQUIRY_DUTY_FSCM

• Click the Rule tab, and then enter the values shown in the following table:
6-14 Oracle Sales Cloud Securing Oracle Sales Cloud

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Set</td>
<td>Multiple Values</td>
</tr>
<tr>
<td>Condition</td>
<td>Access the trading community person for table HZ_PARTIES for all people in the enterprise other than sales accounts and sales prospects. (IMPORTANT: Do not enter directly. Search and select)</td>
</tr>
</tbody>
</table>

- Click the Action tab and move the values View Trading Community Person and Read from the Available Actions list to the Selected Actions list.
- Click **Save**. The confirmation dialog appears. Click **OK**.

7. Create a new duty role to replace Party Information Inquiry Duty (HCM) duty role:

- In the Home page, select HCM in the Application Name list.
- In the Application Roles section, click the **New** action link. The new role tab appears.
- Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>New Party Information Inquiry Duty (HCM)</td>
</tr>
<tr>
<td>Role Name</td>
<td>NEW_PARTY_INFORMATION_INQUIRY_DUTY_HCM</td>
</tr>
<tr>
<td>Description</td>
<td>Views trading community parties other than sales accounts and sales prospects.</td>
</tr>
</tbody>
</table>

- Click **Save**. The new role appears.

8. Create the first data security policy for the new duty role:

- From the top right corner of the role tab, click **Find Policies**.
- Click **Default Policy Domain**. The Search Authorization Policies tab appears.
- Check that the role name appears in the Found Principals list.
- At the bottom section, select the Data Security tab.
- In the Data Security tab toolbar, click the **New** icon. The New Policy tab appears with all fields blank.

- Enter the values shown in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Grant on Trading Community Organization</td>
</tr>
<tr>
<td>DB Resource</td>
<td>Trading Community Person (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
<tr>
<td>Module</td>
<td>Trading Community Model (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
<tr>
<td>Start Date</td>
<td>Use the calendar icon to select yesterday's date.</td>
</tr>
</tbody>
</table>

- Click the Role tab. Check the role name is **NEW_PARTY_INFORMATION_INQUIRY_DUTY_HCM**.

- Click the Rule tab. Enter the values shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Set</td>
<td>Multiple Values</td>
</tr>
<tr>
<td>Condition</td>
<td>Access the trading community person for table HZ_PARTIES for all people in the enterprise other than sales accounts and sales prospects. (IMPORTANT: Do not enter directly. Search and select.)</td>
</tr>
</tbody>
</table>

- Click the Action tab and move the values View Trading Community Organization and Read from the Available Actions list to the Selected Actions list.

- Click **Save**. The confirmation dialog appears. Click **OK**.

9. Create the second data security policy for the new duty role.

- In the Data Security tab toolbar, click the **New** icon. The New Policy tab appears with all fields blank.

- Enter the values shown in the following table:
- Click the Role tab. Check the role name is `NEW_PARTY_INFORMATION_INQUIRY_DUTY_HCM`

- Click the Rule tab, and then enter the values shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Grant on Trading Community Person.</td>
</tr>
<tr>
<td>DB Resource</td>
<td>Trading Community Person (IMPORTANT: Do not enter directly. Search and select)</td>
</tr>
<tr>
<td>Module</td>
<td>Trading Community Model (IMPORTANT: Do not enter directly. Search and select).</td>
</tr>
<tr>
<td>Start Date</td>
<td>Enter yesterday’s date (use the calendar icon).</td>
</tr>
<tr>
<td>Row Set</td>
<td>Multiple Values</td>
</tr>
<tr>
<td>Condition</td>
<td>Access the trading community person for table HZ_PARTIES for all people in the enterprise other than sales accounts and sales prospects. (IMPORTANT: Do not enter directly. Search and select)</td>
</tr>
</tbody>
</table>

- Click the Action tab and move the values View Trading Community Person and Read from the Available Actions list to the Selected Actions list.

- Click **Save**. The confirmation dialog appears. Click **OK**.

**Customizing Security for the Sales Representative Role by Replacing Duty Roles**

1. Replace existing FSCM duty role for Sales Representative with the new roles created.
   - In the Task Bar, set the search parameters to External Roles in Global Scope.
   - Enter Sales Representative in the Search field and click the **Search** icon.
   - From the Search Results list, select Sales Representative.
- Click the folder icon to open the role. A new tab appears for the Sales Representative role.

- Click the Application Role Mapping tab. A list of application groups appears.

- Expand the FSCM node. A list of roles appears under the FSCM node.

- Select the Party Information Inquiry Duty (FSCM) role.

- Click the **Remove Roles** icon. A confirmation dialog appears. Click the **Remove** button.

- Click the **Map** icon. A role search dialog appears.

- Set the search parameters as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>FSCM</td>
</tr>
<tr>
<td>Display Name</td>
<td>New Party Information Inquiry Duty (FSCM)</td>
</tr>
</tbody>
</table>

- Click the **Search** button.

- From the Search Results list, select the New Party Information Inquiry Duty (FSCM) role.

- Click the **Map** button. The role appears under the FSCM node.

- Collapse the node.

2. Replace existing HCM duty role for Sales Representative with the new roles created.

- Expand the HCM node. A list of roles appears under the HCM node.

- Select the Party Information Inquiry Duty (HCM) role.

- Click the **Remove Roles** icon. A confirmation dialog appears. Click the **Remove** button.

- Click the **Map** icon. A role search dialog appears.

- Set the search parameters as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>HCM</td>
</tr>
<tr>
<td>Display Name</td>
<td>New Party Information Inquiry Duty (HCM)</td>
</tr>
</tbody>
</table>
• Click the Search button.

• From the Search Results list, select the New Party Information Inquiry Duty (HCM) role.

• Click the Map button. The role appears under the HCM node.

• Collapse the node.


• In the Task Bar, set the search parameters to Application Roles in CRM.

• Enter Party Information Inquiry Duty in the Search field and click the Search icon.

• From the Search Results list, select Party Information Inquiry Duty.

• Click the folder icon to open the role. A new tab appears for the Party Information Inquiry Duty role.

• From the top right corner of the role tab, click Find Policies.

• Click Default Policy Domain. The Search Authorization Policies tab appears.

• Check that the same role name appears in the Found Principals list.

• At the bottom section, select the Data Security tab.

• In the Data Security locate the following policies:

  Note
  You may have to press F11 on your keyboard to increase the browser height.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Resource Name</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Trading Community Organization, Read</td>
<td>Trading Community Person</td>
<td>All Values</td>
</tr>
</tbody>
</table>

• Select the View Trading Community Organization policy.

• Click the Edit icon. The Edit Policy tab opens.

• Click the Rule tab. Enter the values shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Set</td>
<td>Multiple Values</td>
</tr>
</tbody>
</table>

- In the Task Bar, set the search parameters to Database Resources in Global Scope.
- Enter Trading Community Person in the Search field and click the Search icon.
- From the Search Results list, select Trading Community Person.
- Click the folder icon to open the database resource. A new tab called Edit Database Resource appears for the Trading Community Person and its base table.
- Click the Policy sub-tab. The list of policies is displayed.
- Locate the following policy:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Role</th>
<th>Actions</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant on Trading</td>
<td>HZ_PARTY_INFORMATION_INQUIRY_DUTY</td>
<td>View Trading Community Person, Read</td>
<td>All Values</td>
</tr>
<tr>
<td>Community Person</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Select the policy.
- Click the Delete icon.
- On the right hand side, click the Save button.
- Click the Submit button. The confirmation dialog appears. Click OK.


- In the list of policies for Trading Community Person, locate the following policy:
<table>
<thead>
<tr>
<th>Policy</th>
<th>Role</th>
<th>Actions</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant on Sales</td>
<td>ZCM_SALES_PARTY_REVIEW_DUTY</td>
<td>Read, View Sales Party</td>
<td>Access the sales party for table HZ_PARTIES for all sales accounts in the enterprise.</td>
</tr>
</tbody>
</table>

- Select the policy.
- Click the **Delete** icon.
- On the right hand side, click the **Save** button.
- Click the Submit button. The confirmation dialog appears. Click **OK**.

7. Login to Oracle Sales Cloud using your sales representative credentials.
8. Test the visibility for Accounts for various roles.
Synchronizing User and Role Information with Oracle Identity Management

Synchronization of User and Role Information with Oracle Identity Management: How It Is Processed

Oracle Identity Management (OIM) maintains Lightweight Directory Access Protocol (LDAP) user accounts for users of Oracle Cloud applications. OIM also stores the definitions of abstract roles and job roles, and holds information about roles provisioned to users.

Most changes to user and role information are shared automatically by Oracle Sales and OIM. No action is necessary to make this exchange of information happen.

However, you must run the processes Send Pending LDAP Requests and Retrieve Latest LDAP Changes to manage some types of information exchange between your application and OIM.

The table summarizes the role of each process.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to OIM. The response to each request from OIM to your application indicates transaction status (for example, Completed).</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from OIM that might not have arrived automatically because, for example, there was a failure or error.</td>
</tr>
</tbody>
</table>

This figure summarizes the information flow of the daily processes.
Scheduling the Processes

You must run both processes at least daily to identify and process future-dated changes as soon as they take effect.

Retrieve Latest LDAP Changes must complete before Send Pending LDAP Requests runs. For this reason, leave a gap between the scheduled start times of the processes. Depending on the size of your enterprise and the number of updates, a gap of 1 or 2 hours may be enough.

Send Pending LDAP Requests has two required parameters, **User Type** and **Batch Size**. You’re recommended to use the default values of these parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Type</td>
<td>The types of users to be processed. Values are Person, Party, and All</td>
<td>All</td>
</tr>
<tr>
<td>Batch Size</td>
<td>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 means that the batch size is calculated automatically.</td>
<td>A</td>
</tr>
</tbody>
</table>

Scheduling the LDAP Daily Processes: Procedure

You’re recommended to schedule these processes to run daily:

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to Oracle Identity Management (OIM).</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from OIM that may not have arrived automatically because of a failure or error, for example.</td>
</tr>
</tbody>
</table>
Important
Schedule the processes only when your implementation is complete. Once you schedule the processes, you can't run them on an as-needed basis, which is necessary during implementation.

This procedure explains how to schedule the processes.

Scheduling the Retrieve Latest LDAP Changes Process
1. Select Navigator - Tools - Scheduled Processes to open the Scheduled Processes work area.
2. Click Schedule New Process in the Search Results section of the Scheduled Processes work area.
4. In the Process Details dialog box, click Advanced.
5. On the Schedule tab, select Using a schedule.
6. In the Frequency field, select Daily.
7. Enter the start and end dates and times.
   Plan for Retrieve Latest LDAP Changes to complete before Send Pending LDAP Requests starts.
8. Click Submit.

Scheduling the Send Pending LDAP Requests Process
1. Click Schedule New Process in the Search Results section of the Scheduled Processes work area.
2. Search for and select the process Send Pending LDAP Requests in the Schedule New Process dialog box.
3. In the Process Details dialog box, select a user type value and enter a batch size. You're recommended to leave User Type set to All and Batch Size set to A.
   Click Advanced
4. On the Schedule tab, select Using a schedule.
5. In the Frequency field, select Daily.
6. Enter the start and end dates and times.
   Leave a gap between the start times of the two processes so that Retrieve Latest LDAP Changes completes before Send Pending LDAP Requests starts.
7. Click Submit.

Send Pending LDAP Requests: Explained

It is recommended that you run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to Oracle Identity Management (OIM). Schedule the process in the Scheduled Processes work area.
Send Pending LDAP Requests sends the following items to OIM:

- Requests to create, suspend, and reenable 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 reenable a suspended user account is generated automatically if you rehire a terminated worker.

The process sends these requests to OIM unless the automatic creation and management of user accounts is 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 OIM, which owns them. They're usable only when OIM returns them to Oracle Sales.

- Role provisioning and deprovisioning requests.
  - The process sends these requests to OIM unless automatic role provisioning is disabled for the enterprise.

- Changes to person attributes for individual users.
  - The process sends this information to OIM unless the automatic management of user accounts is disabled for the enterprise.

---

**Note**

All of these items are sent to OIM 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 OIM.

---

**Retrieve Latest LDAP Changes: Explained**


You're recommended to run Retrieve Latest LDAP Changes daily. Schedule the process in the Scheduled Processes work area.

Retrieve Latest LDAP Changes delivers the following information to your application from OIM:

- Names of user accounts.
  - The globally unique identifier (GUID) from the LDAP directory user account is added automatically to the person record.
• Latest information about abstract and job roles.

OIM stores the latest information about all abstract and job roles. Your application keeps a local copy of all role names and types so that lists of roles in user interfaces are up-to-date.

• Work e-mails.

A worker can have only one work e-mail, which OIM owns. Once the e-mail exists, you manage it in OIM. Retrieve Latest LDAP Changes sends any changes to your application.
abstract role
A description of a person’s function in the enterprise that is unrelated to the person’s job (position), such as employee, contingent worker, or line manager. A type of enterprise role.

action
The kind of access named in a security policy, such as view or edit.

condition
An XML filter or SQL predicate WHERE clause in a data security policy that specifies what portions of a database resource are secured.

data dimension
A stripe of data accessed by a data role, such as the data controlled by a business unit.

data role
A role for a defined set of data describing the job a user does within that defined set of data. A data role inherits job or abstract roles and grants entitlement to access data within a specific dimension of data based on data security policies. A type of enterprise role.

data security
The control of access to data. Data security controls what action a user can taken against which data.

data security policy
A grant of entitlement to a role on an object or attribute group for a given condition.

database resource
An applications data object at the instance, instance set, or global level, which is secured by data security policies.

duty role
A group of function and data privileges representing one duty of a job. Duty roles are specific to applications, stored in the policy store, and shared within an Oracle Fusion Applications instance.

enterprise
An organization with one or more legal entities under common control.
**enterprise role**

Abstract, job, and data roles are shared across the enterprise. An enterprise role is an LDAP group. An enterprise role is propagated and synchronized across Oracle Fusion Middleware, where it is considered to be an external role or role not specifically defined within applications.

**enterprise role**

Enterprise roles provide users with access both to the application functions they need to perform their jobs as well as the permissions to access the data where they need to perform those functions. There are two types of enterprise roles: job roles and abstract roles. Job roles permit users to perform activities specific to their job. Abstract roles permit users to perform functions that span the different jobs in the enterprise.

**entitlement**

Grants of access to functions and data. Oracle Fusion Middleware term for privilege.

**function security**

The control of access to a page or a specific widget or functionality within a page. Function security controls what a user can do.

**job role**

A role for a specific job consisting of duties, such as an accounts payable manager or application implementation consultant. A type of enterprise role.

**resource role**

Resource roles indicate the role a resource plays as an individual, or within a resource team.

**role**

Controls access to application functions and data.

**role deprovisioning**

The automatic or manual removal of a role from a user.

**role provisioning**

The automatic or manual allocation of a role to a user.

**security reference implementation**

Predefined function and data security in Oracle Fusion Applications, including role based access control, and policies that protect functions, data, and segregation of duties. The reference implementation supports identity
management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

**segregation of duties**

An internal control to prevent a single individual from performing two or more phases of a business transaction or operation that could result in fraud.

**SQL predicate**

A type of condition using SQL to constrain the data secured by a data security policy.

**work relationship**

An association between a person and a legal employer, where the worker type determines whether the relationship is a nonworker, contingent worker, or employee work relationship.

**XML filter**

A type of condition using XML to constrain the data secured by a data security policy.