# Oracle Fusion Cloud Sales Automation

## How do I create and manage users?

Oracle Fusion Cloud Sales Automation
How do I create and manage users?

G30763-04



Author: Carmen Myrick

# Contents

Get Help i

1 Overview of CX Users and Role Provisioning 1

Types of Sales Users 1
Ways to Create Sales Users 3
Tasks You Accomplish by Creating Users 4
Role Provisioning 6
Role Autoprovisioning 11
Create Additional Resource Roles 12
How can I create rules to automatically provision job roles to sales users? 12
Steps for Setting Up Role Provisioning 14
Edit Your Custom Job or Abstract Roles 15

2 Prepare to Create Users 19

What You Must Do Before Creating Sales Users 19
Create a Resource Organization 20
Designate an Organization as the Top of the Sales Hierarchy 21
Prevent Entry of Duplicate User Email Addresses 22
Create Additional Resource Roles 23
How can I create rules to automatically provision job roles to sales users? 24
How to Configure the Employee Abstract Role for Sales Users 25
Modify the Provisioning Rules for Oracle Sales in the Redwood User Experience 29
Define Rules for Incentive Compensation Abstract Roles 30
Role Provisioning Options 30
Role Autoprovisioning 32
Provision Roles for Testing 33

3 Create Users 37

User Setup Options 37
Create Users 37
Create Restricted Users 40

Configure Administrators to Access Incentive Compensation 41

## 4 User Management 43

Overview of Managing Users 43
Setup Assistant and User Account Preferences 43
Setup Overview 43
Initialize the Security Console 44
The Dos and Don'ts for Using the Security Console 45
User Name and Password Notifications 46
Automatic New Account Notifications and What to Change 47
Set Up Preferences for User Names, Passwords, and Notifications 48
Change User Names 52
Change a User's Email Address 53
Terminate User Accounts 53
Get User Sign-in Sign-out Information 55
Provide Read-Only Access for Individual Users 55
Overview of Managing Passwords 56
Reset Passwords for Other Users 57
View Locked Users and Unlock Users 57

## 5 FAQs for Managing Users 59

What happens when I autoprovision roles for a user? 59
Why did some roles appear automatically? 59
Why can't I see the roles that I want to assign to a user? 59
How do I change user resource roles when job assignments change? 59
How can I change the name of the top resource organization and other resource organizations? 61
How are the records of a terminated employee reassigned? 61
How do I change user resource roles when job assignments change? 62
Can I reactivate a terminated employee record? 63
How can I notify users of their user names and passwords? 63

# Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

## Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

## Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

## Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

## Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

## Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

## Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

# 1 Overview of CX Users and Role Provisioning

## Types of Sales Users

After you've signed up with your Oracle cloud service, you receive the user name and password for one initial user. This topic describes the privileges assigned to the initial user and to each of the different types of sales user that the initial user can create.

> **Note:** These user types are simply suggestions for your configuration. User privileges depend on the job and abstract roles assigned to users. So, for example, you can create a sales user who's also a setup user if you want.

### Initial Users

As an initial user, you can perform many security tasks including creating other users. But you can't perform all the implementation tasks without assigning yourself extra privileges. For example, as an initial user you can submit scheduled processes but can't monitor their statuses.

These are the roles assigned to the initial user:

- Application Implementation Consultant job role: Provides access to all setup tasks across all products.
- IT Security Manager job role: Provides access to security tasks, including the ability to assign other job and abstract roles.
- Application Diagnostic Administrator job role: Provides access to diagnostic tests and data.

The initial user can create each of the types of users described in the rest of this topic.

### Setup Users

You can create setup users and provision them with the same job roles as the initial user so that they can help perform setup tasks. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges.

So that setup users can perform all implementation tasks, in addition to assigning them the same roles as the initial user, you must also provision them with these roles:

- Sales Analyst job role: Makes it possible to create Sales Predictor rules.
- Sales Administrator job role: Lets the setup user perform the typical sales administrator tasks, such as setting up and administering sales territories and processes.
- Employee abstract role: Provides the ability to run and monitor background processes.

Setup users aren't part of the sales organization so they aren't created as resources in the sales application and aren't provisioned with the Resource abstract role. You can't assign sales work to setup users and they can't view sales transaction data or reports. But setup users do have the privileges to assign themselves additional roles to make those tasks possible.

You can find more information about setup users in *Create Implementation (Setup) Users*.

## Sales Administrators

Sales administrators, like other sales application users, are created as resources and are provisioned with job and abstract roles based on the resource role they're assigned. You must create at least one sales administrator user.

Sales administrators are provisioned with the Sales Administrator job role, which includes permissions to manage the import of data from legacy systems, to configure the application according to business needs, and to set up and administer the sales territories and sales processes.

Sales administrator users can view sales transactional data and reports but can't configure sales application security or perform tasks related to an enterprise setup. Sales administrator users are provisioned with these roles:

- Sales Administrator job role
- Resource abstract role
- Employee abstract role

To create sales administrators, follow the procedure outlined in the topic *Create Sales Users*.

## Sales Users

You create Sales users as sales resources. As sales resources, application users can be assigned work and they appear in your sales organization directory.

Sales users are provisioned with job and abstract roles according to the resource role they're assigned. The provisioned job roles don't let sales users do setup tasks, but they can perform functional setups, depending on their role. Provision sales application users with these roles:

- 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

## Sales Restricted Users

To do their jobs effectively, users must be able to view all the data that's relevant to their role. Sometimes users don't need to create, update, or delete that data. You can create users who have privileges to view sales data, but who have limited privileges to change data. You create these users by provisioning these roles:

- Sales Restricted User job role
- Resource abstract role
- Employee abstract role

Users assigned the Sales Restricted User job role can:

- View accounts, contacts, leads, and opportunities.
- Create and modify reports and analytics.
- Update, create and manage service requests.
- Create, update and delete appointments, tasks, and activities for the Activity object.
- Edit forecasts.

Assigning the Sales Restricted User job role to the following types of users provides these users with the visibility into sales data that they require, without assigning them excess privileges.

- Back-office users can view reports, edit forecasts, and view activities.
- Service representatives can view customer information and can see leads and opportunities.
- Seasonal or administrative users can view leads and opportunities.

The Essential User license provides a user with a read-only subscription to Oracle CX Sales and Fusion Service. You must provision the Sales Restricted User job role to users who are assigned an Essential User license.

> **Note:** Some users might require read-only access to application data, but don't need any data update privileges. For example, an auditor who reviews application data for regulatory reasons shouldn't be authorized to change anything. You can assign read-only access to individual users using the Read Only Mode (FND_READ_ONLY_MODE) profile option. For information on how to configure this access for a user, see *Provide Read-Only Access for Individual Users*.

*Related Topics*

- How do I create sales restricted users?
- Provide Read-Only Access for Individual Users
- How do I create application users?
- Create Setup Users
- Give Users the Permission to View All Scheduled Processes

# Ways to Create Sales Users

You can create setup and sales application users in these ways:

- 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 to create setup users and individual Sales users.
- Import users using the Import Management functionality or using the *Quick Import Excel macros* that you download from My Oracle Support.

  Import users if you've many users to create. To import users, you must understand how user attributes are represented in the application and how to map the source attributes to the attributes required by the application. You can't import setup users because the import process requires you to import sales resources. For more information about importing users, see:
  - *Quick Import Excel macros*
  - The topics about importing employee resources in the *Understanding Import and Export Management for Sales and Fusion Service* guide

> **Note:** Don't use the Security Console for creating individual users. You must create sales users as resources who are part of the sales resource hierarchy, and you can't create sales resources in the Security Console. Use the Security Console for user management tasks like resetting user passwords and updating user email addresses.

*Related Topics*

- How do I create application users?

# Tasks You Accomplish by Creating Users

When you create users, several other tasks are automatically performed. For example, users are sent emails with their user names and initial passwords, and the organization chart for your sales organization is built.

Whether or not a task is performed depends on the type of user created, as explained in the following sections.

## Tasks Accomplished for all Users

The tasks in the following table are completed regardless of the type of user you create: setup users, sales administrators, or sales application users. These tasks are performed whether the user is created in the UI or through file import.

| Task Accomplished | More Details |
|---|---|
| Notifies users that their user accounts are created and provides sign-in details. | You can prevent emails from being sent either when creating individual users or by changing the default notification settings as described in the chapter Setting Up Applications Security.<br>The application sends the user notifications only once, either on account creation or later, depending on the setup. |
| Automatically provision the job and abstract roles that provide the security settings users require to do their jobs. | Job and abstract roles are provisioned based on the autoprovisioning rules discussed later in this chapter. |
| Create rudimentary employee records. Employee records are used only if you're also implementing Oracle HCM Cloud, or if you implement it in the future. | You must specify each user either as an employee or as a contingent worker and enter the user's business unit and legal employer. When you create users, the application generates employee records for each user based on your entries. |

## Tasks Accomplished for Resource Users

When you create users as resources by entering resource information for the user, the application also performs the tasks shown in the following table.

**Note:** These tasks don't apply to setup users because they're not created as resources in the organization.

| Task Accomplished | Comments |
|---|---|
| Create resources that can be assigned sales work such as leads, opportunities, and tasks. | Setup users aren't resources in your application and so can't be assigned to sales teams or view reports. |

| Task Accomplished | Comments |
|---|---|
| Create the resource reporting hierarchy used for reporting, forecasting, and work assignments. | When you create a resource, you specify a manager for that resource and build a resource reporting hierarchy. |
| Create resource records that individual users can update with personal information to complete a directory of your organization. | Setup users aren't resources and so their information doesn't appear in your sales organization directory. |
| Create a hierarchy of resource organizations. | 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 aren't resources and so aren't assigned to resource organizations. |

## Resource Reporting Hierarchy

You build a resource reporting hierarchy when you create sales application users by specifying the manager of each user you create, except for the user at the top of the resource hierarchy, for example, the CEO. If you're creating users 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're importing users, then the order doesn't matter provided that all of your users are in the same file.

The resource reporting hierarchy doesn't have to mirror the formal reporting hierarchy, which is captured separately in the Oracle HCM Cloud application if it has been implemented. In Oracle CX Sales and Fusion Service, you can have only one resource reporting hierarchy reporting to one person.

## Resource Organizations and the Resource Organization Hierarchy

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. 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.

In CX Sales and Fusion Service, resource organizations serve a limited purpose. The name of each resource organization appears in the application's Resource Directory, which users can access to obtain information about their coworkers, and in social media interactions. However, resource organizations aren't used in application security or for work assignments. You assign work to individuals rather than their organizations.

You access the Resource Directory from the **Navigator** menu. The resource organization names appear under each person's title. The resource organization names don't have to reflect the names of departments. Departments are tracked along with employee records in the Oracle HCM Cloud application if it has been implemented.

*Related Topics*

- How do I create application users?

# Role Provisioning

Sales users gain access to data and functionality through the job and abstract roles they're assigned. Roles are provisioned to users through predefined role provisioning rules or through provisioning rules that you create.

You can provision both custom and standard job roles using role provisioning rules. Each provisioning rule, also known as a role mapping, defines:

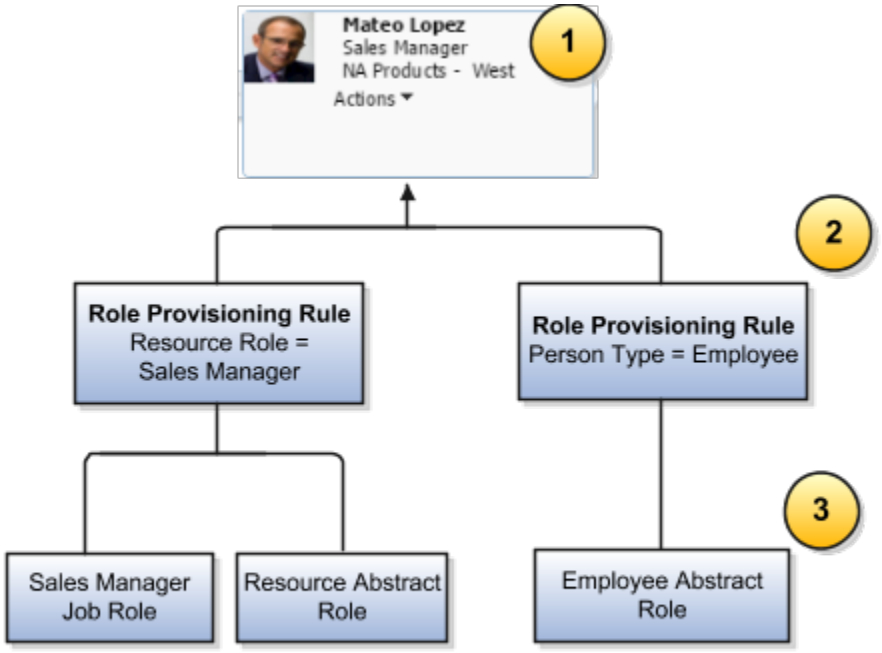
- The job and abstract roles to provision
- The conditions that must exist for the roles to be provisioned
- Whether role provisioning is automatic

  The provisioning rules use resource roles as the condition for provisioning job and abstract roles to sales users. Each provisioning rule can use one resource role, and you assign a resource role to each sales user you create.

  If you select the automatic role provisioning option for a rule, then roles are provisioned automatically when you create the user, if the user matches the rule conditions. It doesn't matter if you create users manually in the UI, or import them from a file or using the Sales User Quick Import Excel macro file. For more information on importing users, start with *Overview of Importing Sales Resources*.

> **Note:** Don't confuse resource roles with job or abstract roles. A user's resource role merely describes the role the user plays in the organization and provides the job title that appears in the company resource directory for the user. Job and abstract roles, on the other hand, provide the user's security permissions.

The following figure provides an example of how role provisioning rules work. When you create the Sales Manager user, you assign that user the Sales Manager resource role provided by Oracle (callout 1), which is the user's title in the organization. You also create the user as an employee person type. The role provisioning rules use the resource role and person type values as conditions. When you create a user as an employee with the Sales Manager resource role, then the conditions are true and the rules automatically assign the user with the Sales Manager job role and the Resource abstract role, and with the Employee abstract role.




## Predefined Sales Resource Roles

Oracle provides you with several standard sales organization resource roles and the appropriate job roles for each of them. The predefined roles include common roles for Oracle Sales and Oracle Fusion Service.

## Predefined Sales Role-Provisioning Rules

Oracle predefines role provisioning rules for provisioning most of the standard Sales and Service job roles. And Oracle supplies rules to assign the Employee abstract role to active users who are created as employees.

Oracle also supplies the Contingent Worker abstract role to active nonemployee users who are created as contingent workers.

The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. You do this step after enabling your Sales or Service offering. If you set up the company information in a different way, perhaps because you're implementing several cloud services at the same time or you're a new customer using the *Setup Assistant*, then you must create the provisioning rules yourself using the steps outlined in *How can I create rules to automatically provision job roles to Sales users?*.

For information about setting up your company information, see *Enter Your Company Information and Corporate Currency*.

The following table lists the role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles the rule provisions. Except for the partner provisioning rules, each rule uses two rule conditions to provision the relevant roles to a user:

- Resource Role or Person Type

  The Resource Role or Person Type condition specifies the job and abstract roles assigned to users.

- HR Assignment Status

  The HR Assignment Status condition ensures that the provisioned job roles are automatically removed if the user is terminated.

  The HR Assignment Status condition doesn't apply to partner users who are created as external sales users. As a result, the partner provisioning rules specify only one condition, Resource Role.

The Requestable, Self-Requestable, and Autoprovision options are enabled for each role assigned by the provisioning rules.

### *Predefined Role-Provisioning Rules*

| Provisioning Rule Name | Condition | Job or Abstract Roles Provisioned |
|---|---|---|
| Channel Account Manager | HR Assignment Status is Active<br>Resource Role is Channel Account Manager | Channel Account Manager<br>Resource |
| Channel Sales Manager | HR Assignment Status is Active<br>Resource Role is Channel Sales Manager | Channel Sales Manager<br>Resource |
| Channel Operations Manager | HR Assignment Status is Active<br>Resource Role is Channel Operations Manager | Channel Operations Manager<br>Resource |
| Chief Executive Officer | HR Assignment Status is Active<br>Resource Role is Chief Executive Officer | Sales VP<br>Resource |
| Contract Administrator | HR Assignment Status is Active<br>Resource Role is Contract Administrator | Contract Administrator<br>Resource |
| Contract Manager | HR Assignment Status is Active<br>Resource Role is Contract Manager | Contract Manager<br>Resource |
| Customer Data Steward | HR Assignment Status is Active<br>Resource Role is Customer Data Steward | Customer Data Steward<br>Resource |
| Data Steward Manager | HR Assignment Status is Active<br>Resource Role is Data Steward Manager | Data Steward Manager<br>Resource |
| Inside Sales Manager | HR Assignment Status is Active<br>Resource Role is CX Inside Sales Manager | Inside Sales Manager<br>Resource |
| Inside Sales Representative | HR Assignment Status is Active | Inside Sales Representative |

| Provisioning Rule Name | Condition | Job or Abstract Roles Provisioned |
|---|---|---|
| | Resource Role is CX Inside Sales Representative | Resource |
| Partner Administrator | Resource Role is Partner Administrator | Partner Administrator |
| Partner Sales Manager | Resource Role is Partner Sales Manager | Partner Sales Manager |
| Partner Sales Representative | Resource Role is Partner Salesperson | Partner Sales Representative |
| Sales Administrator | HR Assignment Status is Active<br>Resource Role is Sales Administrator | Sales Administrator<br>Resource |
| Sales Lead Qualifier | HR Assignment Status is Active<br>Resource Role is Sales Lead Qualifier | Sales Lead Qualifier<br>Resource |
| Sales Manager | HR Assignment Status is Active<br>Resource Role is Sales Manager | Sales Manager<br>Resource |
| Sales Representative | HR Assignment Status is Active<br>Resource Role is Salesperson | Sales Representative<br>Resource |
| Sales Restricted User | HR Assignment Status is Active<br>Resource Role is Sales Restricted User | Sales Restricted User<br>Resource |
| Sales Setup User | HR Assignment Status is Active<br>Resource Role is Sales Setup User | Application Implementation Consultant<br>IT Security Manager<br>Application Diagnostics Administrator<br>Sales Administrator<br>Sales Analyst |
| Sales Vice President | HR Assignment Status is Active<br>Resource Role is Sales Vice President | Sales VP<br>Resource |
| Contingent Worker | HR Assignment Status is Active<br>System Person Type is Contingent Worker | Contingent Worker |
| Employee | HR Assignment Status is Active<br>System Person Type is Employee | Employee |

# Predefined Resource Roles and Provisioning Rules for Oracle Sales in the Redwood User Experience

When you assign these four resource roles to resources, the role provisioning-rules created automatically by the *Setup Assistant* provide access to the Oracle Sales in the Redwood User Experience (Sales in the Redwood UX) UIs.

- Inside Sales Representative
- Inside Sales Manager
- Sales VP
- Sales Administrator

The job roles provisioned by the Sales VP and Sales Administrator provisioning rules provide access to the classic Sales UIs and the Sales in the Redwood UX UIs. Before creating users, edit the Inside Sales Manager and Inside Sales Representative provisioning rules so that they also provide access to the classic Sales UIs.

# Predefined Resource Roles and Provisioning Rules for Fusion Service

Oracle provides resource roles for the Service offering which are used to provision the standard service job roles. Oracle also provides the role provisioning rules for these resource roles so that service users are automatically assigned the job and abstract roles they need.

This table lists the Service role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles each rule provisions:

***Role Provisioning Rules for Fusion Service***

| Provisioning Rule Name | Condition | Job or Abstract Roles Provisioned |
|---|---|---|
| Service Vice President | HR Assignment is Active<br>Resource Role is Service Vice President | Customer Service Manager<br>Resource |
| Service Administrator | HR Assignment is Active<br>Resource Role is Service Administrator | Customer Relationship Management Application Administrator<br>Resource |
| Service Manager | HR Assignment is Active<br>Resource Role is Service Manager | Customer Service Manager<br>Resource |
| Service Representative | HR Assignment is Active<br>Resource Role is Service Representative | Customer Service Representative<br>Resource |

**Note:** If you didn't use the Create Company Information quick setup task to set up your company information, then the predefined role provisioning rules aren't created, and you must create the provisioning rules yourself. For information about creating provisioning rules, see *How can I create rules to automatically provision job roles to sales users?*.

*Related Topics*

- Modify the Provisioning Rules for Oracle Sales in the Redwood User Experience

# Role Autoprovisioning

Autoprovisioning is the automatic allocation or removal of job or abstract roles to users. It occurs for individual users when you create or update the resource role assigned to a user or the user's HR assignment status.

You can also apply auto-provisioning explicitly for the enterprise using the Autoprovision Roles for All Users scheduled process. This topic explains the effects of applying auto-provisioning for the enterprise.

## Roles That Auto-Provisioning Affects

Auto-provisioning applies only to roles that have the **Autoprovision** option enabled in a role mapping.

It doesn't apply to roles without the **Autoprovision** option enabled.

## The Auto-Provision Roles for All Users Scheduled Process

The **Autoprovision Roles for All Users** process compares the roles assigned to a user with all current role mappings.

- Users who satisfy the conditions in a role mapping and who don't currently have the associated roles acquire those roles.
- Users who currently have the roles but no longer satisfy the associated role-mapping conditions lose those roles.

The process creates requests immediately to add or remove roles. These requests are processed by the **Send Pending LDAP Requests** process. When running **Autoprovision Roles for All Users**, you can specify when role requests are to be processed. You can either process them immediately or defer them as a batch to the next run of the **Send Pending LDAP Requests** process. Deferring the processing is better for performance, especially when thousands of role requests may be generated. Set the **Process Generated Role Requests** parameter to **No** to defer the processing. If you process the requests immediately, then **Autoprovision Roles for All Users** produces a report identifying the LDAP request ranges that were generated. Requests are processed on their effective dates.

## When to Run the Process

It's a good idea to run **Autoprovision Roles for All Users** after creating or editing role mappings. You may also have to run it after importing new users to provision roles to the new users. Avoid running the process more than once in any day. Otherwise, the number of role requests that the process generates may slow the provisioning process.

Only one instance of **Autoprovision Roles for All Users** can run at a time.

## Autoprovisioning for Individual Users

You can apply autoprovisioning for individual users on the Create User or Edit User page by clicking **Autoprovision Roles** in the Roles region of the page.

*Related Topics*

- What happens when I autoprovision roles for a user?
- Schedule the Send Pending LDAP Requests Process

# Create Additional Resource Roles

Use these steps to review the resource roles provided by Oracle and to create any additional resource roles you need. Remember that the resource role is only a title. So, if you create a resource role, you must also create the provisioning rule to go with it.

1. Open the task **Manage Resource Roles** from the Setup and Maintenance work area:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Resource Roles
2. To review all the existing resource roles, click **Search** without entering any search criteria.

    All the available resource roles are listed. Roles that are predefined by Oracle are labeled **System**.
3. Here's how to create a resource role:
    a. Click **Create**.
    b. In the **Role Name** field, enter the name of the resource role as you want it to appear in the application UI, for example, `Inside Sales`.
    c. In the **Role Code** field, enter a unique internal name in capital letters. No spaces are permitted, but you can use the underscore character (_) instead. For example, enter `INSIDE_SALES`.
    d. If the resource role belongs to a manager, select the **Manager** option. If the resource role belongs to an individual contributor, such as an inside sales representative, then select the **Member** option.
    e. From the **Role Type** list, select **Sales** to classify the role that you are creating.
4. Click **Save and Close**.

*Related Topics*

- How do I make an employee a sales resource?

# How can I create rules to automatically provision job roles to sales users?

Before you create sales users, review the predefined role provisioning rules used to automatically assign job and abstract roles to users, and create any more rules you need.

For example, you might want to create a new resource role and rule to provision a custom job role you've created.

Oracle provides a role provisioning rule for each of the standard resource roles included with the application. But, you must create role provisioning rules for any new resource roles you create.

The provisioning rules use the resource role that you assign to each sales user as the trigger condition for provisioning job roles.

For all internal sales users, including sales administrators, map the Resource abstract role in addition to the required job roles in the provisioning rule. The Resource abstract role lets users access the Resource Directory. Don't add the Resource abstract role for partner roles.

> **Note:** The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. If you didn't use the Create Company Information quick setup task, then you must create all of these role-provisioning rules manually.

## Review Existing and Create New Provisioning Rules

Use these steps to review existing provisioning rules, and to create new rules:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, to review existing rules:
    a. Search for a role mapping using one of the search fields. For example, to determine if a provisioning rule exists for a resource role, in the Resource Role field, enter the name of a resource role.
    b. Click **Search**.

       If a role provisioning rule exists for the resource role (either a predefined rule or a rule you created), it's displayed in the Search Results area.
    c. To view or edit a provisioning rule, select the rule from the Search Results area.
    d. In the Edit Role Mapping page, review the details for the rule.
3. To create a new provisioning rule, on the Manage Role Mappings page, click **Create**.
4. In the Create Role Mapping page, in the **Mapping Name** field, enter a name that identifies the mapping. For example, if you're creating a rule to provision a resource role you created called Digital Sales Manager, enter `Digital Sales Manager` for the mapping name too.
5. In the Conditions region, enter the conditions shown in this table:

   ***Values to Enter in the Conditions Region***

| Field | Entry |
|---|---|
| Resource Role | Select the resource role you want to provision. For example, select **Digital Sales Manager**. |
| HR Assignment Status | Select **Active**. This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources. |

6. In the Associated Roles region, click **Add** to add the job roles you want to provision.

   For the Digital Sales Manager, for example, you might add the **Sales Manager** job role.

   For internal sales users, add the **Resource** abstract role. Don't add this role for partner roles.

7. For each role you've added, select one or more of the role provisioning options shown in this table:

***Role Provisioning Options***

| Role Provisioning Option | Description |
|---|---|
| Requestable | Qualifying users can provision the role to other users. |
| Self-Requestable | Qualifying users can request the role for themselves. |
| Autoprovision | Qualifying users get the role automatically. |

Qualifying users are users who satisfy the rule conditions.

> **Note:** **Autoprovision** is selected by default. Remember to deselect it if you don't want auto-provisioning.

8. Click **Save and Close**.
9. After creating or editing role mappings, run the scheduled process, Autoprovision Roles for All Users. This process compares all current user role assignments with all current role mappings and creates appropriate auto-provisioning requests.

*Related Topics*

- How do I update existing setup data?

# Steps for Setting Up Role Provisioning

Before you create sales users, there are some role provisioning setup tasks you might have to perform, such as creating additional resource roles or role provisioning rules. These tasks are described in this topic.

## Create Additional Resource Roles

Resource roles are provided for the most commonly used job roles included with the application. Resource role and job role names are the same except for the Salesperson resource role, which provisions the Sales Representative job role, and the Chief Executive Officer resource role, which provisions the Sales Vice President job role. Review the predefined resource roles provided with the application and determine whether or not you require additional resource roles.

You create additional resource roles using the Manage Resource Roles task from the Setup and Maintenance work area in the following circumstances:

- You are creating users with job roles that aren't provided by Oracle, or your organization uses different job titles. For example, you must create a Digital Marketing Manager resource role if you want to include the Digital Marketing Manager title in your organization chart. It's not one of the resource roles created for you.
- You want to provision a user or a subset of users with special privileges. For example, if one of the sales managers in the organization is also in charge of maintaining territories and sales processes, then you create a new resource role that you can provision with both the Sales Manager and the Sales Administrator job roles.

For information on creating additional resource roles, see the topic Create Additional Resource Roles.

## Create Additional Role Provisioning Rules

Predefined role provisioning rules are created automatically when you set up your company information using the Create Company Information quick setup task. A role provisioning rule is provided for the standard resource roles included with the application but you must create provisioning rules for any additional resource roles you create.

When you're creating provisioning rules for users who are sales resources, each rule must provision both the relevant job role and the Resource abstract role. You can assign multiple job roles to an individual. For information about creating provisioning rules, see the topic Create Rules to Automatically Provision Job Roles to Sales Users.

> **Note:** If you didn't use the Create Company Information quick setup task to set up your company information, then the predefined role provisioning rules aren't created; you have to create the provisioning rules yourself. For information about the predefined provisioning rules, see the topic Role Provisioning. For information about setting up your company information, see the Implementing Sales guide.

## Modify Predefined Provisioning Rules

You might have to edit the predefined role provisioning rules in these circumstances:

- If you create custom roles based on the predefined roles, you'll also need to edit the predefined provisioning rules for those roles.

  For example, it's recommended that you use a custom version of the Employee abstract role to avoid unnecessary licensing charges. This means that you'll also need to edit the predefined rule that provisions the Employee role so it provisions the custom role instead. For additional information, see the topic How to Configure the Employee Abstract Role for Sales Users.
- If a predefined provisioning rule doesn't provision all the roles you want to assign to users.

  For example, the Inside Sales Representative and Inside Sales Manager provisioning rules provision users with the roles they need to use the Digital Sales UIs but not with the roles they need to access the CX Sales UIs. Edit these provisioning rules so that they provide users with access to both UIs. For information, see the topic Modify the Provisioning Rules for Digital Sales.

*Related Topics*

- Role Provisioning
- How to Configure the Employee Abstract Role for Sales Users
- Modify the Provisioning Rules for Oracle Sales in the Redwood User Experience
- How can I create rules to automatically provision job roles to sales users?

# Edit Your Custom Job or Abstract Roles

You can create a role by copying a predefined job role or abstract role and then editing the copy.

You must have the IT Security Manager job role to perform this task.

## Edit the Role

To edit a job or abstract role:

1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code. If location-based access is enabled, then you can also manage the Enable Role for Access from All IP Addresses option (see *Overview of Location-Based Access*).
4. Click **Next**.

## Manage Functional Security Privileges

On the Edit Role: Function Security Policies page, any function security privileges granted directly to the copied role appear on the Privileges tab. Click **Load Inherited Policies** to populate the table with privileges that the role inherits. To view details of the code resources that a privilege secures, select the privilege in the Details section of the page.

You can add or delete existing privileges from copied roles but can't create new functional security policies. To delete a privilege that's added directly to the copied role, select the privilege and click the Delete icon. You can't delete inherited privileges.

To add a privilege to the copied role:

1. Click **Add Function Security Policy**.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.

   All the privileges you selected are listed on the Edit Role: Function Security Policies page.
7. Click **Next**.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. Because you can't grant resources directly to roles in the Security Console, only resource grants created before Release 12 appear on this tab. You can't edit these values.

## Manage Data Security Privileges

On the Edit Role: Data Security Policies page, any data security policies granted to the copied role appear. You can add or remove policies from the copied role, or edit the existing policies. For information about creating, editing, and adding data security policies to a role, see *Edit Data Security Policies on the Security Console*.

Click **Next** to continue to the next page.

## Add or Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied role and its inherited duty roles. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the **Delete** icon.

3. Click **OK** to close the confirmation message.

To add a role:

1. Click the **Add Role** icon.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

   The Edit Role: Role Hierarchy page shows the updated role hierarchy.
7. Click **Next**.

## Assign a Role to Users

On the Edit Role: Users page you can assign a copied role to a user.

To remove user access to a role:

1. Select the user in the table.
2. Click the **Delete** icon.
3. Click **OK** to close the confirmation message.

To add user access to a role:

1. Click the **Add User** button.
2. In the Add User dialog box, search for and select a user or role (job or abstract role).
3. If you select a role, then click **Add Selected Users** to add all the users assigned the role to your custom role. If you select a single user, then click **Add User to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional users.
6. Close the **Add User** dialog box. The Edit Role: User page shows the updated role membership.
7. Click **Next**.

## Review a Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Then do this:

1. Click **Back** to make corrections.
2. When you've completed any corrections required, click **Save and Close** to save the role.
3. Click **OK** to close the confirmation message.

The role is available immediately.

*Related Topics*

- Copy Job or Abstract Roles
- Edit Data Security Policies on the Security Console

# 2 Prepare to Create Users

## What You Must Do Before Creating Sales Users

There are some preliminary tasks you need to do before you start creating sales users.

When you create sales users, you not only provision the permissions the sales users need to do their jobs, but you also build the organization chart for your sales organization. This practice applies to both creating users via import or directly in the UI.

This means that you must set up any additional role provisioning rules you need, as well as the elements that the application uses to create the organization chart in the Resource Directory, such as the root of the organization chart, and the names of the roles the resources play in the organization.

You're getting ready to create two types of sales users:

- Sales team members without any sales application administration duties. These include salespeople, sales managers, and sales vice presidents.
- At least one sales administrator user who will set up and administer the sales territories and sales processes.

### Setup Overview

Before creating sales users, make sure that you've completed the following tasks:

1. Create any additional resource roles you need.

   You must assign a resource role (a name describing the role each resource plays in the organization) to each sales user you create. The resource roles display 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 information about creating resource roles, see *Create Additional Resource Roles*.
2. Create a resource organization for each of the manager users you create, including the top manager in your hierarchy.

   You can use the Manage Internal Resource Organizations task to create each resource organization. For details, see *Create a Resource Organization*. Alternatively, you can create each resource organization as you create each manager user in the UI or when you import the user. Individual contributors who aren't managers inherit the organization assigned to their managers.

   As you create users, the application creates an organization hierarchy that you can use to browse through the sales organization's resource directory.
3. You can explicitly designate the resource organization you create for the top manager in your organization as the top of your organization tree by using the Manage Resource Organization Hierarchies task. For details, see *Designate an Organization as the Top of the Sales Hierarchy*.

   If you don't specify the top organization, the application automatically builds the resource organization hierarchy based on the management hierarchy you specify when you create users. You must enter a manager for each user you create, except for the manager at the top of the resource hierarchy.

4. Decide what job roles you want to assign to your users and determine whether or not you need to create any custom roles. For example, it's recommended that you provision sales users with a custom version of the Employee abstract role. For information, see *How to Configure the Employee Abstract Role for Sales Users*.

   Remember that you aren't restricted to assigning one job role to a user. For example, you might want to provision the sales manager in charge of setting up sales territories and sales processes with the Sales Administrator job role in addition to the Sales Manager job role. Assigning both job roles allows 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. If you created additional resource roles, then create the provisioning rules to automatically provision the appropriate job roles and abstract roles to users who are assigned those resource roles. You must create a provisioning rule for every resource role you use.

   For information about creating provisioning rules, see *Create Rules to Automatically Provision Job Roles to Sales Users*.
6. Enable duplicate checking for the email addresses you enter while creating users in the UI.
7. When you create users, the application sends emails with the sign-in credentials to the new users unless you disable notifications. You can configure this behavior as described in *User Name and Password Notifications*.

## How Setup Assistant Gets You Ready to Create Sales Users

If you used the *Setup Assistant* to help you complete the initial implementation of the Sales offering, then some of the tasks described in the previous section are already completed for you. Here are some of the things Setup Assistant does:

- Creates the role-provisioning rules for the standard resource roles provided by Oracle.
- Creates additional resource roles. All you do is enter their names.
- Creates the role-provisioning rules to provision the job and abstract roles you specify for those additional resource roles.
- Creates the user at the top of the resource organization, and the name of the resource organization, if you enter these values.
- Prevents you from accidentally entering duplicate email addresses for users by setting the profile option *Enable Validation of User Work Email*.

# Create a Resource Organization

Create a resource organization for every manager in your sales organization, including the top manager, usually the CEO. Use the procedure in this topic if you want to create your resource organization hierarchy before you create users.

Alternatively, you can create resource organizations while you're creating manager users in the UI or when you import them. When you import users from a file, you can create the resource organizations automatically from the information you include in the file itself.

## Creating the Resource Organization

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

- Functional Area: Users and Security
- Task: Manage Internal Resource Organizations

2. On the Manage Internal Resource Organizations page, click the **Create** icon.

   The Create Organization: Select Creation Method page is displayed.
3. Select **Option 2: Create New Organization**, then click **Next**.
4. Enter the name of the resource organization in the **Name** field, for example, **Vision Corp**. This name is shown in the resource directory.

   Here are a few things to keep in mind when naming resource organizations:

   - Each resource organization name must be unique.
   - The names don't have to correspond to any formal organization in your enterprise. The names are there solely to create a resource directory.
   - Don't use the name of a manager as the organization name as you might want to reassign the organization to someone else later.
5. In the Organization Usages region, click the **Add** icon and select **Sales Organization**.
6. Click **Finish**.

   If you need to change the name of a resource organization at a later date, you can do so using the Manage Internal Resource Organizations task. For details, see the FAQ in this chapter: How can I change the name of the top resource organization and other resource organizations?

*Related Topics*

- How can I change the name of the top resource organization and other resource organizations?
- How do I update existing setup data?

# Designate an Organization as the Top of the Sales Hierarchy

After you create the resource organization for the top person in the sales organization hierarchy, for example, the CEO, you can designate that resource organization as the top organization in the sales hierarchy.

If you don't explicitly designate the top organization, the application automatically builds the resource organization hierarchy based on the management hierarchy you specify when you create users. You must enter a manager for each user you create, except for the manager at the top of the resource hierarchy.

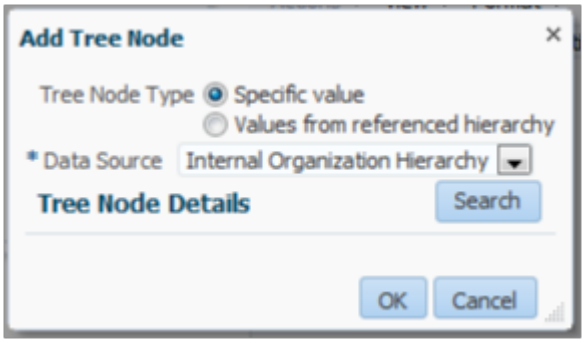
## Designating the Top of the Sales Hierarchy

Here are the steps to designate a resource organization as the top of the sales hierarchy:

1. Navigate to Setup and Maintenance and go to: **Sales offering** > **Users and Security functional area** > **Manage Resource Organization Hierarchies task**.
2. On the Manage Resource Organization Hierarchies page, search for and select **Internal Resource Organization Hierarchy**. This value is supplied by Oracle.
3. The appears.

4. In the View Organization Hierarchy: Internal Resource Organization Hierarchy page, select **Edit This Hierarchy Version** from the Actions menu.
5. In the Edit Organization Hierarchy Version page, click **Add** in the Internal Resource Organization Hierarchy region.

   The Add Tree Node window appears, as shown in this sample screenshot:




6. Click **Search**.
7. Click **Search** again in the Search Node window.
8. In the Search Results list, select the resource organization that you created for the top person in the hierarchy.
9. Click **OK**.
10. In the Edit Organization Hierarchy Version page, save your work and close the page.
11. If a warning appears, click **Yes**.

*Related Topics*

- How do I update existing setup data?

# Prevent Entry of Duplicate User Email Addresses

Enable email validation to prevent entering duplicate email addresses when you create or edit users.

After you enable validation, a warning message is displayed listing the owner of the email address if you enter a duplicate value. Having this warning gives you the opportunity to enter a unique email before saving the user's record. Email validation on the Create User and Edit User pages is disabled by default. Follow the steps in this topic to enable validation.

**Note:** User import includes its own separate duplicate checking which is enabled by default.

## Set the Profile Option

To enable email validation, you set the profile option PER_MANAGE_USERS_EMAIL_VALIDATION.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Sales Foundation
   - Task: Manage Administrator Profile Values

2. On the Manage Administrator Profile Values page, enter **PER_MANAGE_USERS_EMAIL_VALIDATION** in the **Profile Option Code** field and click **Search**.
3. In the Profile Values section of the search results, enter **Y** in the **Profile Value** field.
4. Click **Save and Close**.

**Note:** When email validation is enabled, it applies to the Create User and Edit User pages. It doesn't apply to user accounts that you manage on the Security Console.

# Create Additional Resource Roles

Use these steps to review the resource roles provided by Oracle and to create any additional resource roles you need.

Remember that the resource role is only a title. So, if you create a resource role, you must also create the provisioning rule to go with it.

## Create a Resource Role

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Resource Roles
2. On the Manage Resource Roles page, review the existing resource roles by clicking **Search** without entering any search criteria.

    All the available resource roles are listed. Roles that are predefined by Oracle are labeled **System**.
3. To create a new resource role, click **Create**.

    The Create Role page appears.
4. In the **Role Name** field, enter the name of the resource role as you want it to appear in the application UI, for example, `Digital Sales Manager`.
5. In the **Role Code** field, enter a unique internal name in capital letters. No spaces are permitted but you can use the underscore character instead. For example, enter `DIGITAL_SALES_MANAGER`. If you're importing users from a file then you must include this code in your file rather than the name.
6. If the resource role belongs to a manager, select the **Manager** option. If the resource role belongs to an individual contributor, select the **Member** option.
7. From the **Role Type** list, select **Sales** to classify the role that you're creating.
8. Click **Save and Close**.

*Related Topics*

- How do I update existing setup data?

# How can I create rules to automatically provision job roles to sales users?

Before you create sales users, review the predefined role provisioning rules used to automatically assign job and abstract roles to users, and create any more rules you need.

For example, you might want to create a new resource role and rule to provision a custom job role you've created.

Oracle provides a role provisioning rule for each of the standard resource roles included with the application. But, you must create role provisioning rules for any new resource roles you create.

The provisioning rules use the resource role that you assign to each sales user as the trigger condition for provisioning job roles.

For all internal sales users, including sales administrators, map the Resource abstract role in addition to the required job roles in the provisioning rule. The Resource abstract role lets users access the Resource Directory. Don't add the Resource abstract role for partner roles.

> **Note:** The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. If you didn't use the Create Company Information quick setup task, then you must create all of these role-provisioning rules manually.

## Review Existing and Create New Provisioning Rules

Use these steps to review existing provisioning rules, and to create new rules:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, to review existing rules:
    a. Search for a role mapping using one of the search fields. For example, to determine if a provisioning rule exists for a resource role, in the Resource Role field, enter the name of a resource role.
    b. Click **Search**.

       If a role provisioning rule exists for the resource role (either a predefined rule or a rule you created), it's displayed in the Search Results area.
    c. To view or edit a provisioning rule, select the rule from the Search Results area.
    d. In the Edit Role Mapping page, review the details for the rule.
3. To create a new provisioning rule, on the Manage Role Mappings page, click **Create**.
4. In the Create Role Mapping page, in the **Mapping Name** field, enter a name that identifies the mapping. For example, if you're creating a rule to provision a resource role you created called Digital Sales Manager, enter `Digital Sales Manager` for the mapping name too.

5. In the Conditions region, enter the conditions shown in this table:

***Values to Enter in the Conditions Region***

| Field | Entry |
|---|---|
| Resource Role | Select the resource role you want to provision. For example, select **Digital Sales Manager**. |
| HR Assignment Status | Select **Active**. This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources. |

6. In the Associated Roles region, click **Add** to add the job roles you want to provision.

   For the Digital Sales Manager, for example, you might add the **Sales Manager** job role.

   For internal sales users, add the **Resource** abstract role. Don't add this role for partner roles.
7. For each role you've added, select one or more of the role provisioning options shown in this table:

***Role Provisioning Options***

| Role Provisioning Option | Description |
|---|---|
| Requestable | Qualifying users can provision the role to other users. |
| Self-Requestable | Qualifying users can request the role for themselves. |
| Autoprovision | Qualifying users get the role automatically. |

   Qualifying users are users who satisfy the rule conditions.

   **Note: Autoprovision** is selected by default. Remember to deselect it if you don't want auto-provisioning.
8. Click **Save and Close**.
9. After creating or editing role mappings, run the scheduled process, Autoprovision Roles for All Users. This process compares all current user role assignments with all current role mappings and creates appropriate auto-provisioning requests.

*Related Topics*

- How do I update existing setup data?

# How to Configure the Employee Abstract Role for Sales Users

The Employee abstract role is assigned to all sales users who are employees but many of the privileges it provides aren't required if you've implemented only CX Sales.

Although these privileges aren't used, they can incur licensing charges. For this reason, Oracle recommends that you create a custom version of the Employee role that doesn't include these unnecessary privileges and provision the custom role to your sales users. This task involves these steps.

- Copy the predefined Employee role to create a custom version of the role.

  See the topic: *Create a Custom Employee Role for Sales Users*.
- Edit the custom employee role to remove unnecessary privileges.

  See the topic: *How do I remove unneeded privileges from my custom employee abstract role?*.
- Edit the predefined Employee provisioning rule so that it assigns the custom employee role instead of the predefined Employee role to all users created as employees.

  Test the changes you've made to the rule and then implement it for all your users. See the topic: *Provision the Custom Employee Role to Users*.

# Create a Custom Employee Role for Sales Users

Create a custom employee abstract role that contains only the privileges sales users require using these steps.

1. Sign in to the sales application as a user who has the IT Security Manager job role.
2. Navigate to the Security Console (**Navigator** > **Tools** > **Security Console**).
3. On the Roles tab, search for and select the Employee abstract role (ORA_PER_EMPLOYEE_ABSTRACT).
4. In the search results, select **Copy Role** from the **Actions** menu of the Employee role.
5. In the Copy Options dialog box, select the **Copy top role and inherited roles** option, then click **Copy Role**.

   > **Note:** When you select the **Copy top role and inherited roles** option, you copy not only the role you've selected, but also all of the roles in its hierarchy. When inherited duty roles are copied, you can edit them without affecting other roles in the source role hierarchy.

6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab, but you can overwrite these values for the role that you're copying. For example, you might want to name the role **Employee Custom Sales**. Any roles inherited by the copied role are unaffected by any name changes that you make here.
7. Click **Next**.
8. Click the Summary train stop.
9. On the Summary page, click **Submit and Close**, then click **OK** to close the confirmation message.
10. Review the progress of your role copy operation on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

# How do I remove unneeded privileges from my custom employee abstract role?

By default, some privileges are assigned to the Employee abstract role that aren't used by Sales users. You can delete these privileges from the custom employee role you previously created.

To delete privileges that are assigned directly to the custom employee role, edit the custom employee role you created. If a privilege is inherited from a duty in the custom employee role hierarchy, you've to edit the custom duty role to remove the privilege.

1. On the Roles tab of the Security Console, search for and select the custom employee role you've just created, for example, **Employee Custom Sales**.
2. In the search results, select the **Edit Role** option from the **Actions** menu of the Employee Custom Sales role.
3. Click **Next**.

   On the Edit Role: Function Security Policies page, all the privileges assigned directly to the Employee Custom Sales role are listed.
4. To display the privileges the custom employee role inherits from duty roles in its hierarchy, scroll to the end of the page, then click **Load Inherited Policies**.

   All the privileges the custom employee role has are now listed:
   - If the **Inherited from Role** column is blank for a privilege, the privilege is assigned directly to the employee custom role and can be deleted on this page.
   - If the **Inherited from Role** column isn't blank, you have to edit the custom duty role listed to delete a privilege from it.
5. Delete the privileges that are assigned directly to the Employee Custom Sales role that aren't required for sales users.
   a. Delete the following privileges by selecting each privilege in turn, then clicking **Delete**.
      - Manage Reputation Scores (HWR_REPUTATION_EE_PRIV)
      - Manage Social Roles (HWR_SOCIAL_ROLES_EE_PRIV)
   b. Click **Yes** in the Warning dialog box to confirm the deletion.
   c. Click the Summary train stop.
   d. On the Edit Role: Summary page, verify both privileges you deleted are listed as Removed in the Function Security Policies row, click **Save and Close**, then click **OK**.
6. Now delete the excess privileges that are inherited by the Employee Custom Sales role from duty roles in its hierarchy.
   a. On the Roles tab of the Security Console, edit each duty role shown in the table and remove the privilege listed.

   > **Note:** The default prefix and suffix for copied roles is specified on the Roles subtab of the Security Console Administration tab. By default, the role-name suffix is Custom but this might differ in your environment.

| Privilege to Remove | Custom Duty Role to Edit |
|---|---|
| Manage Expense Report | Expense Entry Custom |
| Create Performance Document by Worker | Performance Management Worker Custom |
| Provide Performance Evaluation Feedback | Performance Management Worker Custom |
| View Performance Information on Worker Dashboard | Performance Management Worker Custom |
| Access Time Work Area | Time and Labor Worker Custom |

| Privilege to Remove | Custom Duty Role to Edit |
|---|---|
| Manage Requisition | Requisition Self Service User Custom |
| Access Learning Common Components | Access Learning Common Components Custom |

b. Once you've deleted each privilege, review your changes to the custom duty role on the Edit Role Summary page and save them.

7. Finally, edit the Employee Custom Sales role on the Security Console.

   Navigate to the Function Security Policies page and verify that all the excess privileges, both those assigned directly to the role and those inherited from other roles in the hierarchy, have been removed.

# Provision the Custom Employee Role to Users

Modify the predefined provisioning rule for the Employee abstract role so that it assigns users the custom employee role you created instead of the predefined Employee role. Test your configuration for an individual user, then apply the change to all users.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
2. On the Role Mappings page, enter **Employee** in the **Mapping Name** field, then click **Search**.
3. In the Search Results area, click the **Employee** mapping.
4. On the Edit Role Mapping: Employee page, make the following change in the Associated Roles region:
   a. Select the Employee row, then click the Remove icon to remove the predefined Employee role.
   b. Click the Add Row icon to add a new row.
   c. In the **Role Name** field, search for your custom employee abstract role, for example, **Employee Custom Sales**, then add the role.
   d. Select the **Autoprovision** option for the role.
   e. Click **Save and Close**, then click **OK**.
5. Click **Done** on the Role Mappings page.
6. Test that the role provisioning rule updates are working correctly for a single employee user:
   a. Open the Search Person page ( **Navigator** > **My Team** > **Users and Roles**).
   b. Search for and select a user who was created as an employee person type.

      The Edit User page for the user opens.
   c. In the Roles region, click **Autoprovision Roles**. Any roles for which the user qualifies automatically appear in the Role Requests table with the status **Add Requested**. Your custom employee role, Employee Custom Sales, should be listed.

      > **Note:** If the Employee role was initially provisioned to a user manually rather than through automatic role provisioning, the change to the provisioning rule won't remove the original Employee role from the user.

   d. Click **Save and Close**.

7. Now navigate to the Scheduled Processes work area (**Navigator** > **Tools** > **Scheduled Processes** ) and run the **Autoprovision Roles for All Users** process.

   This process compares all current user role assignments with all current role mappings and creates appropriate autoprovisioning requests. The process can take some time to complete depending on the number of users impacted.

# Modify the Provisioning Rules for Oracle Sales in the Redwood User Experience

Modify the predefined role-provisioning rules for the Inside Sales Representative and Inside Sales Manager job roles to give sales users all the permissions they need to do their work in both Oracle Sales in the Redwood User Experience and classic Sales UIs.

Users who want to work in both the Digital Sales UIs and the CX Sales UIs must have two job roles: one to provide access to Digital Sales (Inside Sales Manager or Inside Sales Representative), and one to provide access to CX Sales (Sales Manager or Sales Representative).

The predefined Inside Sales Manager and Inside Sales Representative role provisioning rules only provision the Digital Sales job roles, but you can edit the rules so that they also provision the CX Sales roles. Here's what you have to do.

1. Sign in as a setup user or the initial user you received when you signed up with Oracle.
2. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
3. On the Role Mappings page, search for the role mapping for the CX Inside Sales Manager resource role:
   a. In the Search region, click the **Resource Role** list.
   b. Search for and select the `cx Inside Sales Manager` resource role.
   c. Click **Search**.

   The Search Results display the mappings for the CX Inside Sales Manager resource role.
4. Click the mapping name and make the following edits:
   a. On the Edit Role mapping page, in the Associated Roles region, click **Add Row** (the plus sign icon).
   b. In the new row, search for and add the **Sales Manager** job role.
   c. Select the **Autoprovision** option for the role.
   d. Click **Save and Close**.
5. Repeat step 3 for the CX Inside Sales Representative resource role.
6. Repeat step 4 to add the Sales Representative job role to the provisioning rule for the CX Inside Sales Representative resource role.
7. When you are finished, click **Done**.

**Results:**

Any users assigned the CX Inside Sales Manager or CX Inside Sales Representative resource roles are now automatically provisioned with both job roles they need.

# Define Rules for Incentive Compensation Abstract Roles

You can define rules to assign the Incentive Compensation Participant and Incentive Compensation Participant Manager abstract roles to salespeople. You can either create new provisioning rules or modify the existing rules. In this procedure, you modify the existing rule.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. In the Manage Role Mappings page search area, select the **Salesperson** resource role and click **Search**.
3. You see two Sales Representative mapping names, and you modify both. Click one of them.
4. In the Conditions region, you see the resource role is Salesperson.
5. In the Associated Roles region, the associated roles include Resource and Sales Representative. If these are also correct for your participant role, then click **Add**.
6. Search for and select the **Incentive Compensation Participant** abstract role.
7. Click **OK**.
8. Select whether you want to autoprovision the roles or have them be requested.
9. Save.

To map the Incentive Compensation Participant Manager role:

1. Search for **Sales Manager** in the Resource Role field.
2. Choose the Sales Manager role. It has the Sales Manager and Resource associated roles.
3. Click **Add**.
4. Search for and select the **Incentive Compensation Participant Manager** abstract role.
5. Click **OK**.
6. Save and close.

# Role Provisioning Options

Job and abstract roles are assigned to users by defining a relationship, called a mapping or provisioning rule, between the role and some conditions. Users who satisfy the rule conditions are eligible to acquire the roles specified in the rule.

Predefined provisioning rules are provided with the application but you can also create new rules using the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area. This topic describes role mapping options for automatic and manual role provisioning.

> **Note:** All role provisioning generates requests to provision roles. Only when those requests are processed successfully is role provisioning complete.

# Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

- The user meets the conditions defined in the rule.
- You select the **Autoprovision** option for the role specified in the rule.

For example, to create a role provisioning rule that automatically provisions the Resource abstract role and the Sales Manager job role to users assigned a resource role, Digital Sales Manager, that you previously created, perform these steps:

1. Specify these conditions for the rule.

| Field | Value |
|---|---|
| **Resource Role** | Digital Sales Manager |
| **HR Assignment Status** | Active |

2. Specify the **Resource** abstract role and the **Sales Manager** job role for the provisioning rule, and select the **Autoprovision** option for each.

Users who match the conditions acquire the roles automatically when you either create or update the resource role or HR assignment status values for a user. The provisioning process also removes automatically provisioned roles from users who no longer satisfy the role-mapping conditions.

# Manual Provisioning of Roles to Users

Users, such as sales managers or administrators, can provision roles manually to other users if:

- The user meets the conditions defined in the rule.
- You select the **Requestable** option for the role in the provisioning rule.

Users can also request a role when managing their own accounts if:

- The user meets the conditions defined in the rule.
- You select the **Self-requestable** option for the role in the provisioning rule.

For example, to create a role provisioning rule to assign roles to each active employee who has been assigned a resource role, Sales Operations Manager, that you previously created, perform these steps.

1. Specify these conditions for the rule.

| Field | Value |
|---|---|
| **Resource Role** | Sales Operations Manager |
| **HR Assignment Status** | Active |

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

2. Specify these roles for the rule.

| Role | Option |
|---|---|
| **Resource** | Autoprovision |
| **Sales Administrator** | Autoprovision |
| **Customer Data Steward** | Requestable |
| **Sales Representative** | Self-requestable |

In this example, when you assign the Sales Operations Manager resource role to a user, the user:

- Is automatically provisioned with the Resource and Sales Administrator roles when you click the Autoprovision Roles option on the Create User or Edit User page
- Can grant the Customer Data Steward role to other users
- Can request the Sales Representative job role

Users keep manually provisioned roles until the user is terminated or the role is deprovisioned manually.

## Role-Provisioning Rule Names

Use unique names for your provisioning rules and devise a naming scheme that shows the scope of each role mapping. For example, a provisioning rule named CEO Autoprovisioned Roles could include all roles provisioned automatically to resources assigned the CEO resource role.

*Related Topics*

- Role Autoprovisioning

# Role Autoprovisioning

Autoprovisioning is the automatic allocation or removal of job or abstract roles to users. It occurs for individual users when you create or update the resource role assigned to a user or the user's HR assignment status.

You can also apply auto-provisioning explicitly for the enterprise using the Autoprovision Roles for All Users scheduled process. This topic explains the effects of applying auto-provisioning for the enterprise.

## Roles That Auto-Provisioning Affects

Auto-provisioning applies only to roles that have the **Autoprovision** option enabled in a role mapping.

It doesn't apply to roles without the **Autoprovision** option enabled.

## The Auto-Provision Roles for All Users Scheduled Process

The **Autoprovision Roles for All Users** process compares the roles assigned to a user with all current role mappings.

- Users who satisfy the conditions in a role mapping and who don't currently have the associated roles acquire those roles.
- Users who currently have the roles but no longer satisfy the associated role-mapping conditions lose those roles.

The process creates requests immediately to add or remove roles. These requests are processed by the **Send Pending LDAP Requests** process. When running **Autoprovision Roles for All Users**, you can specify when role requests are to be processed. You can either process them immediately or defer them as a batch to the next run of the **Send Pending LDAP Requests** process. Deferring the processing is better for performance, especially when thousands of role requests may be generated. Set the **Process Generated Role Requests** parameter to **No** to defer the processing. If you process the requests immediately, then **Autoprovision Roles for All Users** produces a report identifying the LDAP request ranges that were generated. Requests are processed on their effective dates.

## When to Run the Process

It's a good idea to run **Autoprovision Roles for All Users** after creating or editing role mappings. You may also have to run it after importing new users to provision roles to the new users. Avoid running the process more than once in any day. Otherwise, the number of role requests that the process generates may slow the provisioning process.

Only one instance of **Autoprovision Roles for All Users** can run at a time.

## Autoprovisioning for Individual Users

You can apply autoprovisioning for individual users on the Create User or Edit User page by clicking **Autoprovision Roles** in the Roles region of the page.

*Related Topics*

- What happens when I autoprovision roles for a user?
- Schedule the Send Pending LDAP Requests Process

# Provision Roles for Testing

## What's Required for Testing Configurations in the Sandbox

If you're creating configurations for a specific job role or creating your own custom objects, then you must be provisioned with additional job roles to view and test those configurations in the sandbox.

Enable the testing of both types of configurations using the steps described in this section.

## What's Required for Role-Specific Configurations

If you're creating configurations for a specific job role in either Application Composer or Page Composer, then you must assign yourself that same job role to be able to test the configurations in the sandbox. For example, if you're creating your own page layout for the Sales Manager job role, then you must have the Sales Manager job role to view and test the layout. If you later create a different layout for salespeople, then you must deprovision the Sales Manager job role and provision yourself with the Sales Representative job role instead.

## What's Required for the Objects You Create

If you're creating your own objects, then you must assign yourself the Custom Objects Administration (ORA_CRM_EXTN_ROLE) role. The application automatically generates this object role the first time you create an object in the application. Unless users have this role, they can't view or test the objects they create.

## Setup Overview

1. While signed in as a setup user or the initial user you received when you signed up with Oracle, edit the role-provisioning rule for sales administrators and add the required job roles. Here is a summary of the steps:
    a. In the Setup and Maintenance work area, use the following:
        - Offering: Sales
        - Functional Area: Users and Security
        - Task: Manage HCM Role Provisioning Rules
    b. Search for all role-provisioning rules containing the Sales Administrator job role.
    c. For each rule, you add the job roles required for testing. Selecting the **Self-requestable** option makes it possible for individual users to assign themselves each job role when needed.
    d. If you're creating custom objects, then you must also add the Custom Objects Administration role. You must select both the **Self-requestable** and the **Autoprovision** option for this role. This object role is required for all objects you create, so you want to provision it automatically for future to sales administrators.
2. Sales administrators, who are resources with the Sales Administrator job role, navigate to the Resource Directory and assign themselves the job roles they need. Setup users, who are not resources, can edit their own user records in the Manage Users work area and assign themselves the roles there.

    For details on how resources can assign themselves job roles in the Resource Directory, see the Assign Yourself an Additional Job Role topic.

*Related Topics*

- Assign Yourself Additional Job Roles Required for Testing
- Enable Sales Administrators to Test Configurations in the Sandbox
- Enter Setup Data Using Assigned Tasks

# Enable Sales Administrators to Test Configurations in the Sandbox

Modify the security role-provisioning rules to make it possible for administrators to assign themselves the job roles they need for testing custom configurations in the sandbox.

For viewing and testing the custom objects they create, administrators must have the Custom Objects Administration (ORA_CRM_EXTN_ROLE) role. To test job role-specific configurations, they must have the same job role. In this example, we are looking at sales administrators.

## Modify the Provisioning Rule for Sales Administrators

1. Sign in as a setup user or the initial user you received when you signed up with Oracle.
2. In the Setup and Maintenance work area, use the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
3. On the Manage Role Mappings page, search for the role mapping for sales administrators:
    a. In the Search region, click the **Role Name** list and select the **Search** link.
    b. In the Search and Select window, enter `Sales Administrator` in the **Role Name** field and click **Search**.
    c. Select the role name and click **OK**.
    d. Click **Search**.
4. On the Manage Role Mapping page, click **Search**.

    The Search Results display the mappings with the Sales Administrator job role.
5. Click the mapping name of each mapping and make the following edits:
    a. In the Associated Roles region, click **Add Row** (the plus sign icon) and add the job roles required for testing.
    b. For each job role, select the **Requestable** and the **Self-requestable** options and deselect **Autoprovision**. You don't want the job roles assigned to the sales administrators automatically.
    c. If you're creating your own objects, then you must also add the Custom Objects Administration role. The application automatically generates this object role the first time you create an object. For this job role select all of the options: **Requestable**, **Self-requestable**, and **Autoprovision**. All users creating their own objects must have this role.
    d. Click **Save and Close**.
6. When you have added the job roles to all the provisioning rules, click **Done**.

*Related Topics*

- Assign Yourself Additional Job Roles Required for Testing
- Enter Setup Data Using Assigned Tasks

# Assign Yourself Additional Job Roles Required for Testing

Administrators can use the procedure in this topic to assign themselves the roles they need to test role-specific modifications in the sandbox.

For example, if you're a sales administrator testing UI modifications for sales managers, you must assign yourself the Sales Manager job role. If you're creating your own custom objects, you must assign yourself the Custom Objects Administration role, if this role isn't already assigned to you. The Custom Objects Administration role is required for testing your objects in the sandbox.

> **Note:** You can only assign yourself job roles that are made self-requestable in the role-provisioning rules created by a setup user. A setup user has the privileges to create other users and manage application security.

1. Navigate to the **Resource Directory**.
2. Select **View Resource Details** from the **Actions** menu in your record.
3. On the Resource page, click the Roles tab.
4. Click **Add Role**.
5. In the Add Role window, search for the role you want to use for testing by name or partial name, select it, and click **OK**.

   For testing objects you created, you must add the Custom Objects Administration role.

   > **Note:** Available roles include only those that were set up as self-requestable during provisioning rule setup.

   The application returns you to the Resource page and displays the requested role in the Roles Requests region.
6. You can remove a role you no longer need for testing by selecting it and clicking **Remove**.
7. Click **Save and Close**.

   The new role becomes available for your use in a few minutes, pending the completion of a background process. The role displays in the Current Roles region the next time you navigate to this page.

# 3 Create Users

## User Setup Options

There are a number of different options you can use to control default functionality when users are created in the application. Review the user setup options described here and make any configuration changes you want before you start creating users.

### User Name and Password Notifications

By default, users automatically receive an email notification containing their sign-in details when their user account is created. Oracle provides sample notifications but you can edit the text of the email notifications, create your own notifications, or suppress email notifications altogether.

### Password Policy

During implementation, you set the password policy for the enterprise. For example, you can configure how complex passwords must be, when they expire, and when a user is notified that a password is about to expire. By default, the application requires passwords with eight letters and one number but you may want stronger passwords.

### Default User Name Format

You can select the default format used to generate user names for users in cases where a user name isn't specified. Unless you specify otherwise, the default format is email address.

You can review user setup options by navigating to the Administration tab of the Security Console. For detailed information about configuring each of these options, see the chapter Setting Up Applications Security.

*Related Topics*

- User Name and Password Notifications
- Set the Default User Name Format
- Password Policy

## Create Users

You must create sales users as resources who are part of the sales resource hierarchy. You can create sales users either in the Manage Users task UI or by resource import, but you can't create resources in the Security Console.

Before creating application users, make sure you've completed these tasks:

- Set up any additional resource roles or role provisioning rules that are required.

- Create a resource organization for each manager. If you don't create the resource organization ahead of time, then you must do so while creating each manager user.

  Each manager is assigned a resource organization. Individual contributors automatically inherit their manager's resource organization. The application determines who's a manager from the resource role you assign to the 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, first create the user at the top of the hierarchy and that user's organization. You don't enter a manager for this user. You can then create the rest of the users starting directly under the top of the hierarchy and working your way down.

See these playbooks for more information:

- *How do I get started with Oracle Sales in the Redwood User Experience?*
- *What are the basic security concepts and procedures for Oracle CX?*
- *How do I create and manage users?*

## Create an Application User

Here's how to create sales users in the UI. The procedure is slightly different for managers and individual contributors:

- You must assign each manager to a resource organization. You can create the resource organization while creating the manager.
- Individual contributors automatically inherit their managers' resource organization.

The application determines who's a manager from the resource role you assign to the user.

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
2. In the Search Results section, click the **Create** icon.
3. In the Create User page, Personal Details region, enter the user's name and a unique email address. The application sends user notifications to this email address by default unless you disable notifications in the Security Console.

   > **Note:** After you create the user, if you want to change the email address you can do so on the Users tab of the Security Console or using file import. You can't change email addresses on the Edit User page of the Manage Users work area.

4. The application prefills today's date in the Hire Date field and uses that date as the start date for the resource.

   If you're planning to use quotas, then you must make sure that the hire date is a date before the start of the first quota period. For example, if you're allocating monthly quotas for fiscal year July 01, 2024 to June 30, 2025, then you must enter a hire date of `7-1-2024` or earlier.

   > **CAUTION:** You can't change the hire date after you create the user.

5. In the User Details region, you can either create a new account or link an existing, standalone user account to the new person record you're creating.
   - When creating sales users, create a new account. To create a new account, select the **Enter user name** option and then enter a user name. If you leave the User Name field blank, then the user name is generated automatically using the enterprise default format. Unless you specify otherwise, email address is the default user name format.

- Alternatively, if you want to link the new person record you're creating to an existing standalone user account, select the **Link user account** option, then search for and select the user account in the **Link User Account** dialog box.

6. In the User Notification Preferences region, select the **Send user name and password** option if you want a notification to be sent to the user when you save the user record and the user account is created. The notification includes a URL users can use to reset their password and sign in.

   The **Send user name and password** option is enabled only if notifications are enabled on the Security Console and an appropriate notification template exists. For example, if the predefined notification template **New Account Template** is enabled, then a notification is sent to the new user when you select the **Send user name and password** option.

   If you deselect the **Send user name and password** option, a notification isn't sent when the account is created but you can choose to send the email later by running the Send User Name and Password E-Mail Notifications process. The process sends notifications to any users for whom you haven't so far requested an email. An appropriate notification template must be enabled at that time. Alternatively, you can use the Security Console to reset the password and send the notification.
7. In the Employment Information region, enter the values shown in the following table.
8. ***Employment Information Region Entries***

| Field | Entry |
|---|---|
| **Person Type** | Select Employee. |
| **Legal Employer** | Select the legal employer Oracle created using the information you provided when you signed up with the cloud service. |
| **Business Unit** | Select the business unit for the user. Oracle creates an initial business unit using the information you provided when you signed up. |

   You don't need to complete the remaining fields in the Employment Information region.
9. In the Resource Information region, enter the following values.

   ***Resource Information Region Entries***

| Field | Entry |
|---|---|
| **Resource Role** | Select the role the user plays in the resource organization. |
| **Reporting Manager** | Select the user's manager.<br><br>If you're creating the top user in your hierarchy, such as the CEO, you can leave this field blank. |
| **Organization** | If the user you're creating is a manager, and if you already created a resource organization for this manager, then select the appropriate resource organization. If you haven't created a resource organization for the manager, then you can create one by clicking the **Create** link from |

| Field | Entry |
|---|---|
| | the end of the **Organization** list. The **Create Organization** dialog box is displayed allowing you to enter a new organization name.<br><br>If the user you're creating isn't a manager, then the resource organization is automatically copied from the manager. |

10. In the Roles region, click **Autoprovision Roles**.

    Any roles for which the user qualifies automatically appear in the Role Requests table with the status **Add Requested**.

    The application provisions roles according to the provisioning rules specified for the selected resource role. Each sales user must have both the Employee and the Resource abstract roles in addition to the job roles they require.
11. You can also provision a role manually to the user if required by clicking **Add Role**. The **Add Role** dialog box opens.
12. Search for and select the role. The role is added to the Role Requests table with the status **Add Requested**.

    > **Note:** Roles that you can provision to others must appear in a role mapping for which you satisfy the role-mapping conditions and where the **Requestable** option is selected for the role.

13. Click **Save and Close**.

    The application creates the user. If you selected the **Send user name and password** option, the application also sends the user the email with the URL the user can use to sign in to the application for the first time.
14. Click **Done**.

*Related Topics*

- Types of Sales Users
- Create a Resource Organization

# Create Restricted Users

You can create sales application users who have extensive privileges to view sales data, but limited privileges to create, update, or delete that data, by assigning users the Sales Restricted User job role.

For example, you might want to assign the Sales Restricted User job role to accounting or legal users, to seasonal or administrative users, or to users who are assigned an Essential User license. The Essential User license provides a user with a read-only subscription to the cloud service.

Use these steps to create a sales restricted user.

1. Create the user who's to have restricted access to the application.

   For information about this task, see the topic, *How do I create application users?*.
2. When creating the user, specify these values.

| Field | Value |
|---|---|
| **Person Type** | Employee |
| **Resource Role** | Sales Restricted User |

3. In the Roles region, click **Autoprovision Roles**.

   The user is automatically assigned the following roles:

   - Sales Restricted User job role
   - Resource abstract role
   - Employee abstract role

     A predefined rule automatically assigns the Employee abstract role to all active users who are created as employees.

# Configure Administrators to Access Incentive Compensation

Use this procedure to create administrators who have access to the Incentive Compensation application.

1. Create provisioning rules that create a mapping between attributes of your person and the security role to be automatically assigned. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, enter a name for your mapping.
3. There isn't a resource role that qualifies as an Incentive Compensation Administrator, so typically mappings use job roles. In the Conditions region, select a job role that was configured in Human Capital Management. For example, Incentive Compensation Analyst. Add any other conditions you want to use to select individuals to be assigned roles.
4. In the Associated Roles region, click **Add Row**.
5. Search for and select the role you want to assign to people who match your mapping conditions. These are the available Incentive Compensation roles:

   - Incentive Compensation Analyst
   - Incentive Compensation Plan Administrator
   - Incentive Compensation Manager
6. Save and close.
7. After users are assigned to an Incentive Compensation security role, they also need access to Incentive Compensation business units. In the Setup and Maintenance work area, go to the following:

- Offering: Sales
- Functional Area: Incentives
- Task: Manage Business Unit Data Access for Users

8. In the Manage Data Access for Users page, click **Create**.
9. Select a user name and role.
10. The security context must be Business Unit.
11. Select the name of the business unit in the Security Context Value field.
12. Save and close.
13. Create data access records for each role and business unit combination for this user.

# 4 User Management

## Overview of Managing Users

Once you create users and provision them with access to the application, there are various user management tasks you have to perform on an on-going basis. Here are examples of some of the tasks you might have to do:

- Assigning different resource roles to users when they change jobs within the organization or are promoted
- Terminating user accounts when users leave the organization
- Acting as a proxy for users so you can troubleshoot issues

This chapter describes how to perform these and other user management tasks using the sales application UI. But you can also use file import functionality to perform user management tasks such as:

- Making changes to employee resource information, for example, name or email address
- Enabling or disabling user accounts
- Making promotion, demotion, or transfer updates for an employee resource

For additional information, see the chapter about importing resource data in the guide Understanding Import and Export Management for Sales and Fusion Service at http://docs.oracle.com.

## Setup Assistant and User Account Preferences

Setup Assistant uses the default settings when creating setup users and the CEO at the top of the resource hierarchy. You can change the default behavior for the rest of your setup.

Here are the default settings:

- User names are set to email addresses.
- Passwords must be at least 8 characters long and include a number
- The application automatically notifies users when their accounts are created, when passwords need to be changed, and so on

## Setup Overview

Review the settings for user name format and password strength and set up notifications before you create users. By default, the application uses the email address to create user names and requires passwords with eight letters and one number.

You may want shorter user names and stronger passwords. You must also create your own versions of the notifications users receive regarding their accounts. Oracle provides sample notifications, but they include Oracle-specific language and may not include all of the information users need.

The Security Console that you use for all these tasks includes many advanced features. Some don't even apply to your sales application. So, limit your use of the Security Console to the scope listed here.

Here's a list of the setup tasks covered in this chapter. You can open the tasks from the Setup and Maintenance work area, Sales offering, and Users and Security functional area. Remember that you may have to show All Tasks to see the task that you want.

| Step | Applies To | Description | Navigation | Where to Get More Details |
|---|---|---|---|---|
| 1 | Both Digital Sales and CX Sales | Initialize the Security Console. | **Setup and Maintenance** > **Sales** > **Users and Security** > **Import Users and Roles into Application Security** | See the topic: *Initialize the Security Console* |
| 2 | Both Digital Sales and CX Sales | Set up preferences for user name format, passwords, and create your own versions of the notifications that users receive about their accounts and passwords. | **Setup and Maintenance** > **Sales** > **Users and Security** > **Manage Applications Security Preferences**, then select the **User Categories** tab. | To understand the notification process for new accounts and recommendations on the kinds of notification changes you may want to make, see the topic: *Automatic New Account Notifications and What to Change*<br><br>For setup instructions, including a list of tokens you can use in your notifications, see the topic: *Set Up Preferences for User Names, Passwords, and Notifications* |

*Related Topics*

- Automatic New Account Notifications and What to Change
- Set Up Preferences for User Names, Passwords, and Notifications

# Initialize the Security Console

You must initialize the Security Console before using it for the first time by running the process Import Users and Roles into Application Security. The process copies users, roles, privileges, and data security policies from the LDAP directory, policy store, and Applications Core Grants schema to Oracle Fusion Applications Security tables. Having this information in the tables makes the search feature of the Security Console fast and reliable. After the process completes the first time, Oracle recommends that you schedule the process to run daily.

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

- Show: All Tasks
- Task: Import Users and Roles into Application Security

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

   This action starts the Import User and Role Application Security Data process. After the process completes, you can use the Security Console.
3. Now set up this same process to run daily:

   a. On the Import Users and Roles into Application Security page, click **Advanced**.
   b. Click the **Schedule** tab.
   c. Select the Using a schedule option.
   d. From the **Frequency** list, select **Daily**.
   e. Enter an end date far in the future.
   f. Click **Submit**.

# The Dos and Don'ts for Using the Security Console

The Security Console is a powerful tool, but you don't need all of its power for your initial setup. Here's an overview of the Security Console tabs and their uses. Only setup users, or other users with the IT Security Manager job role, can access the Security Console.

| Tab | Dos and Don'ts |
|---|---|
| Roles | Create your own roles as described in Securing Sales and Service guide. |
| Users | • Don't create users or provision job roles here. For sales, you must create users as resources using the Manage Users task, resource import, and REST web services. Follow the instructions in the rest of this guide to create users and provision job roles. If you do create user accounts in the Security Console, then you must create the users again as resources using the Manage Users task and link the accounts you created in the Create Users page.<br>• Use this tab only to manage user passwords and update user email addresses. Note that all users, even members of the sales organization who can't access the Security Console, can reset their own passwords. That's done by clicking the user name in the welcome page and selecting the Preferences option from the Settings and Actions menu.<br>• While you can use this tab to change user names, doing so requires some extra setup for Oracle BI Answers, the embedded reporting tool for building and modifying reports. Oracle BI Answers creates a separate GUID from the user ID when you create a user. If you change the user ID, then you must update the BI Answers GUID by running the Rename Accounts Self-Service utility. You can download the utility from My Oracle Support, article Oracle Fusion BI: Self Service Forget Accounts and Rename Accounts Tools (Doc ID 2635720.1). |
| Analytics | Review role assignments and compare roles. This advanced security functionality is covered in the Securing Sales and Service guide. |
| Certificates | The sales application doesn't use this functionality. |
| User Categories | Specify password policies and manage notifications users receive about their accounts and passwords. You can specify different behavior for different categories of users. For the sales application, all the |

| Tab | Dos and Don'ts |
|---|---|
| | users you create are initially assigned to the Default category. But you can create additional user categories and move users to them. |
| Single Sign-On | Configure single sign-on. |
| API Authentication | Used for defining JSON Web Tokens other applications can use to validate themselves with Oracle CX Sales and Fusion Service. |
| Administration | Use to set role copying preferences and other advanced features covered in the Securing Sales and Service guide. |

You can find information about more advanced tasks, including security configuration, in the Securing Sales and Service and the Extending Sales and Service guides.

# User Name and Password Notifications

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

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

## Predefined Notification Templates

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

***Predefined Notification Templates***

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

| Notification Template | Description |
|---|---|
| Password Reset Confirmation Template | Notifies the user when a password has been reset. |
| New Account Template | Notifies a user when a user account is created and provides a reset-password link. |
| New Account Manager Template | Notifies the user's manager when a user account is created. |

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

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

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

# Automatic New Account Notifications and What to Change

For security reasons, users get the sign-in information they need to start using the application in two separate notifications. The first email tells users an account was created for them and includes a link they can use to create their passwords. The second email, which confirms the password reset, includes the user name.

Here's how the process works by default:

1. The application sends the new account notification. The email includes only the link to reset your password. It doesn't list the user name.
2. Users click the link in the email and create their passwords.
3. If users already know their user names, they can sign in to the application right away.
4. The application sends the second password reset confirmation, which includes the user name.
5. If users don't know their user names, they can get the user names from the second notification.

You can view the default notification text by opening the two templates provided by Oracle: ORA New Account Template and ORA Password Reset Confirmation Template in the Security Console. When you create your own templates, the text of the Oracle notification templates is copied automatically to your new template. You can edit the text or replace it with your own.

As set up by Oracle, the application also notifies the user's manager when a user account gets created and when passwords get reset. If you don't want to spam sales managers, you can disable these notifications or replace them with text of your own.

## Suggested Changes

At a minimum, change the text of sample notifications to replace Oracle-specific language. You may also want to clarify the process:

- New Account Template:

  Add language that makes it clear that to users that they can get the user name from the notification they receive immediately after they create their passwords.

- Password Reset Confirmation Template

  Modify the text to highlight the user name, so it's easy to spot in the email. When making the edits, remember that users receive this notification every time they reset their passwords, not just the first time they create their password.

For navigation and setup details, including available tokens, see the topic: Set Up Preferences for User Names, Passwords, and Notifications.

*Related Topics*

- Set Up Preferences for User Names, Passwords, and Notifications

# Set Up Preferences for User Names, Passwords, and Notifications

Use the Security Console to set your preferences for user names, passwords, and user notifications. For example, you can require users to set stronger passwords, implement shorter user names, change the text of the notifications your users receive, or turn notifications off completely.

Oracle provides only sample notifications. You must change the Oracle-specific language in the notifications and add additional information users may need. For example, the initial notification users receive about their new account includes a link to create your password. But, for security reasons, Oracle doesn't include the user name. In that initial new account notification, you may want to explain that you get the user name from the subsequent password reset confirmation.

## Set Preferences for User Names and Passwords

1. Open the Security Console from the Setup and Maintenance work area:
   - Offering: Sales
   - Functional Area: Users and Security
   - Show: All Tasks
   - Task: Manage Applications Security Preferences

   Alternatively, click **Tools** > **Security Console** on the home page.

2. Click **User Categories**.

   On the User Categories tab, you can set up different preferences and notifications for different categories of users. Since all of the sales users you create and import are created in the Default category, you set preferences for that category only.
3. Click **DEFAULT**.

   On the DEFAULT User Category: Details page, you can set the user-name format.
4. Click **Edit**.
5. Select the user-name format you want to use from the **User Name Generation Rule** list.

   The application uses your selection to generate user names unless you enter the user names manually or import them from a file. By default, the application uses the email address as the user name.

   If you're implementing Partner Relationship Management, then you must use email for creating partner contacts. Otherwise, you can use any of the three following options:

   - First name.last name
   - Email
   - First initial and last name

   Don't use **Person or party number** because numbers aren't easily remembered by users. For example, if the person number generated by the application for John Smith is 100000000178803, then the user name is 100000000178803 as well.
6. Selecting the **Generate system user name when generation rule fails** option ensures that the application generates a user name even if there is no information available for the option you selected.
7. Click **Save and Close**.
8. Click the **Password Policy** subtab.
9. Here you can specify password strength and expiration. For example, you can require users to use special characters in passwords and specify how frequently passwords must be changed.
10. Selecting the **Administrator Can Manually Reset Password** option, makes it possible for administrators to manually create new passwords for users.
11. Click **Save and Close**.

## Configure Email Notifications and Change the Oracle-Specific Text

In the Notifications subtab on the DEFAULT User Category tab, you can specify which email notifications, if any, are sent to users and the text of those notifications. At present, the application supports text-only notifications in one language.

You can make these changes:

- Turn all notifications on or off.

  By default, all notifications are turned on. If you're setting up a test environment, turn off notifications while creating sales users to prevent the users from signing in to the application while you're setting it up.
- Turn individual notifications on or off.

  By default, all individual notifications are turned on.
- Create your own notifications.

  Oracle provides predefined English-language sample templates with Oracle-specific language. You must create your own templates to provide users with the information they need.

Here's how to configure the email notifications:

1. Click the **Notifications** subtab.

   The subtab lists the default notification templates provided by Oracle. The list includes the events that trigger the notifications and the email subject lines.
2. To make changes, click **Edit**.
3. If you want to turn off all notifications, then deselect the **Enable Notifications** option under the **Notification Preferences** heading.
4. If you want to turn off individual notifications, then:

   a. Click the template name link.
   b. Deselect the **Enabled** check box.
   c. Click **Save and Close**.
5. Here's how to create your own notification templates:

   a. Click **Add Template** and select the event.

      Selecting the event automatically copies over the text provided in the corresponding Oracle template, which you can then edit.
   b. Edit the notification subject line and text.

      Here's a list of the tokens you can include in the message text. Each token must be within curly brackets and preceded by a dollar sign, for example: `${firstName}`.

| Token | Meaning | Events |
|---|---|---|
| userLoginId | User name | - Forgot user name<br>- Password expired<br>- Password reset confirmation |
| firstName | User's first name | All events |
| lastName | User's last name | All events |
| managerFirstName | Manager's first name | - New account created - manager<br>- Password reset confirmation - manager<br>- Password reset - manager |
| managerLastName | Manager's last name | - New account created - manager<br>- Password reset confirmation - manager<br>- Password reset - manager |
| loginURL | URL where the user can sign in | - Expiring external IDP signing certificate<br>- Password expired<br>- Password expiry warning |

| Token | Meaning | Events |
|---|---|---|
| resetURL | URL where the user can reset his or her password | - New account created - manager<br>- New user created<br>- Password generated<br>- Password reset<br>- Password reset - manager |
| CRLFX | New line | All events |
| SP4 | Four spaces | All events |
| adminActivityUrl | URL where an administrator initiates an administration activity | Administration activity requested |
| providerName | External identity provider | Expiring external IDP signing certificate |
| signingCertDN | Signing certificate | Expiring external IDP signing certificate |
| signingCertExpiration | Signing certificate expiration date | - Expiring external IDP signing certificate<br>- Expiring service provider signing certificate |
| encryptionCertExpiration | Encryption certificate expiration date | Expiring service provider encryption certificate |
| adminFirstName | Administrator's first name | - Administration activity location-based access disabled confirmation<br>- Administration activity single sign-on disabled confirmation |
| adminLastName | Administrator's last name | - Administration activity location based access disabled confirmation<br>- Administration activity single sign-on disabled confirmation |

c. Select the **Enabled** option.
d. Click **Save and Close**.

The predefined template provided by Oracle is automatically disabled. You can only have one template for each event.

6. On the DEFAULT Category: Notifications page, click **Done**.

## Set the Synchronization Process Frequency Warning

If you don't like warning messages, read on. Whenever you navigate to the Security Console, you get a warning if the Import User and Role Application Security Data process was not run in the last six hours. If you scheduled the process to run daily, then it makes good sense to change the value of the warning as well.

1. Click the **Administration** subtab.
2. Change the value for the **Hours Since Last Synchronization Job Run Warning**.

*Related Topics*

- Automatic New Account Notifications and What to Change

# Change User Names

User names are automatically generated in the enterprise default format when you create a new user if you don't manually specify a user name. The default format is the user's email address, but you can change this value.

For example, you might choose to use first name.last name as the default format. You can also manually override an individual user's existing user name, if necessary.

> **CAUTION:** Although you can change the user name of an existing user, changing it isn't a good idea. Changing the user name requires extra setup for Oracle BI Answers. Oracle BI Answers, the embedded reporting tool for building and modifying reports, creates a separate GUID from the user name when you create a user. If you change the user name, then you must update the BI Answers GUID by running the Rename Accounts Self-Service utility. You can download the utility from My Oracle Support article Oracle Fusion BI: Self-Service Forget Accounts and Rename Accounts Tools (Doc ID 2635720.1). If you used the user name in any script, then you must update that script as well.

To change an existing user name, sign in to the application as a setup user, then perform these steps.

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.

   You can also search for the Manage Users task in the Setup and Maintenance work area.
2. Search for and select the user whose user name you want to change.

   The Edit User page for the user opens.
3. In the User Details region, enter the new user name in the **User Name** field.

   You can enter the user name in any format you choose.
4. Click **Save and Close**.

   The updated name is sent automatically to your LDAP directory server.

   The user's password and roles remain the same.

When you change an existing user name on the Edit User page, the user doesn't receive an automatic notification of the change. So it's a good idea to send details of the updated user name directly to the user.

# Change a User's Email Address

To change sales users' email addresses, use the same import process that you used to create them. You can also use REST services. This setup applies to both CX Sales and Digital Sales.

You can also use these steps to change email addresses on the Users tab in the Security Console work area. However, this method is not always foolproof:

1. Open the Security Console by clicking the **Security Console** link under the **Tools** heading in the Navigator.
2. Click the **Users** tab.
3. Search for the user using one of the following:
    - First or last name, but not both
    - User name
4. Click the user name link.
5. On the User Account Details window, click **Edit**.
6. In the Edit User Account window, edit the email address.

> **Note:** Don't edit any of the other information available on the Edit User Account page. Use the Manage Users task instead.

7. Click **Save and Close**.

*Related Topics*

- What can I use the Security Console for?

# Terminate User Accounts

This topic describes how you can terminate a user account when an employee leaves your company. You can't delete a sales user account using the Security Console. But when an employee leaves your company, you can suspend the user account by completing these steps.

1. Do either one of these tasks:
    - Inactivate the user's account.
    - Remove the user's roles.
2. Set an end date for the resource.

The process outlined in this topic applies if you're using only Oracle CX Sales and Fusion Service. If your company also uses Oracle HCM Cloud, then a different process applies.

> **Note:** When you deactivate a user account, the user record isn't deleted from the application. You can still view a deactivated user's record in the Manage Users work area.

## Inactivating a User Account

When an employee leaves your company, in most cases it's best practice to inactivate the user account. Inactivating the user's account prevents the user from being able to log in to the application.

These are the steps to inactivate a user account.

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
2. On the Search Person page, search for and select the user whose account you want to inactivate. The Edit User page for the user opens.
3. In the User Details section, in the **Active** field, select **Inactive**.
4. Click **Save and Close**.

## Removing Roles from a User

Instead of inactivating a 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 specific pages you have created.

These are the steps to selectively remove roles from a user.

1. Navigate to the Search Person 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** icon. 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.

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

These are the steps to set the end date for a user.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Resources
2. On the Manage Resources page, search for and select the resource you want to edit. The Resource page for the individual opens.
3. With the Organization tab selected, select the **Edit** option from the **Actions** menu.

   The Edit Organization Membership page opens.
4. In the **To Date** field, enter the date the individual is leaving the company.
5. Click **Save and Close**.

When the end date you specify for a resource arrives, this is what happens:

- 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 aren't automatically removed but you can remove them manually.
- Resource roles for the individual are deprovisioned.
- If the terminated individual had any reports, they're reassigned to his or her manager.

*Related Topics*

- How do I update existing setup data?

# Get User Sign-in Sign-out Information

You can get the last seven days of user sign-in sign-out information using a setting available on the Add User Account page in Security Console. To view the setting, you must enable a profile option.

You can access the sign-in sign-out information through REST APIs. For more information, see the topic Sign In and Sign Out Audit REST Endpoints in *REST API for Common Features in Oracle Fusion Cloud Applications* on the Oracle Help Center.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**:
   ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the **Profile Value** drop-down list, select **Yes**.
4. Click Save and Close.

**Note:** The audit data is available for seven days.

The profile option is enabled. On the Add User Account page in Security Console, the setting to get user sign-in sign-out information appears now in the Advanced Information section.

On the Security Console, click **Users**. On the User Accounts page, click **Add User Account** and select **Enable Administration Access for Sign In-Sign Out Audit REST API**. You can also enable this option on the User Account Details Edit page.

# Provide Read-Only Access for Individual Users

Some users may need read-only access to Oracle CX Sales and Fusion Service applications. For example:

- A service representative must replicate a user's transaction without saving any changes.
- An auditor reviews application data for regulatory reasons but isn't authorized to change anything.

Read-only access is controlled by the Read Only Mode (FND_READ_ONLY_MODE) profile option. This topic describes how to set Read Only Mode to all Oracle CX applications for specific users.

## Set the Read Only Mode Profile Option

To enable read-only mode for a user:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. In the Search section of the Manage Administrator Profile Values page, enter **FND_READ_ONLY_MODE** in the **Profile Option Code** field and click **Search**.
3. In the FND_READ_ONLY_MODE: Profile Values section of the page, click the **New** icon.
4. In the new row of the profile values table:
    a. Set **Profile Level** to **User**.
    b. In the **User Name** field, search for and select the user.
    c. Set **Profile Value** to **Enabled** to activate read-only access for the selected user.
5. Click **Save and Close**.

When the user next signs in, a page banner reminds the user that read-only mode is in effect. The user can edit values in the application but can't update or save any changes they make.

# Overview of Managing Passwords

There are a number of password management tasks you may have to perform either when you're setting up your application or on an on-going basis. Here are some examples.

***Password Management Tasks***

| Task | Where to Get More Details |
|---|---|
| Define the password policy for a user category if you don't want to implement the default policy. | • *Password Policy*<br>• *Configure a Custom Password Policy*<br>• *Password Expiry Report* |
| Configure the email notifications sent to users when password-related events occur, such as when a user's password expires. | *User Name and Password Notifications* |
| Reset passwords for users. | *Reset Passwords for Other Users* |
| Enable users who are locked out of the application to sign in again. | View Locked Users and Unlock Users in this chapter.*Password Expiry Report* |
| Review password changes for your users. | *User Password Changes Audit Report* |

**Note:** All users can request new passwords for themselves by selecting the **Forgot Password** link on the application Sign In page, or by selecting the **Password** option on the Preferences page. To navigate to the Preferences page, click your user image or name in the global header to open the **Settings and Actions** menu, then select the **Set Preferences** option.

# Reset Passwords for Other Users

Use the Security Console to reset passwords for other users. Only setup users, and other users with the IT Security Manager job role, can access the Security Console.

> **Note:** All users can reset their own passwords by clicking their user name or image in the global header and then selecting the **Set Preferences** link in the **Settings and Actions** menu. They can also reset their passwords by using **Forgot Password** on the sign-in page.

1. Navigate to the Security Console **Navigator** > **Tools** > **Security Console**.
2. In the Security Console, click the **Users** tab.
3. On the User Accounts page, search for the user using one of these values:
    - First or last name, but not both
    - User name
4. From the **Action** menu for the user, select **Reset Password**.

   The Reset Password window is displayed showing the password strength policy.
5. If you want the application to send an email to users with a link that they can use to create their own passwords, then select the **Automatically generate password** option.
6. Use these steps to reset the password yourself:
    a. Select the **Manually change the password** option.
    b. Enter the new password twice.

    > **Note:** The option to reset a password manually is only available if you select the option **Administrator can manually reset password** on the Password Policy subtab of the User Categories page on the Security Console.
7. Click **Reset Password**.

*Related Topics*

- How do I update existing setup data?

# View Locked Users and Unlock Users

A user gets locked in the application on entering incorrect password for multiple times. The locked users report provides the list of locked users for both these scenarios.

You can get a list of locked users using the Locked Users scheduled process. You can then manually unlock the users using the Security Console. Only an administration user with the IT Security Manager job role can run the locked users report.

# View Locked Users

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search and select the **Locked Users** process and click **OK**.
3. In the Process Details dialog box, click **Submit**.
4. Click **OK** in the confirmation message dialog box.
5. Click **Succeeded** for the selected Locked Users report.
6. In the **Log and Output** section, click **Attachment** to download the report spreadsheet.

   The spreadsheet shows the list of users who are locked.

The Locked Users spreadsheet contains the following two tabs:

- LOCKED_USERS_<Request ID> - This tab contains the list of locked and active users who can't sign in to the application because of locked status.
- LOCKED_AND_INACTIVE_USERS_<Request ID> - This tab contains list of locked and inactive users who can't sign in to the application because of locked and inactive status.

# Unlock Users

1. On the Security Console, click **Users**.
2. From the **Search** drop-down list, select **Locked Users** and click the search icon.

   All the locked users are displayed.
3. Click the display name of a user to view the details.
4. Click **Edit**.
5. In the Account Information section, deselect **Locked**.
6. Click **Save and Close**.
7. Click **Done**.

   The user is unlocked and can sign in to the application.

# 5 FAQs for Managing Users

## What happens when I autoprovision roles for a user?

The role-provisioning process reviews the user's assignments against all current role mappings. The following changes are made to the user's roles:

- The user acquires any role he or she qualifies for but doesn't have
- The user loses any role he or she no longer qualifies for

It's a good idea to autoprovision roles to individual users on the Edit User page when there are new or changed role mappings. Otherwise, no automatic updating of roles occurs until you next update the user's assignments.

## Why did some roles appear automatically?

In a role mapping:

- The conditions specified for the role match the user's assignment attributes, such as job.
- The role has the **Autoprovision** option selected.

## Why can't I see the roles that I want to assign to a user?

You can see the roles that you want to assign, if the role satisfies all of the following conditions:

- A role mapping exists for the role. For more information on creating a role mapping, see the topic *Create a Role Mapping*.
- The Requestable option is selected for the role in the role mapping. For more information, see the topic *How do I provision HCM data roles to users?*.
- At least one of your assignments satisfies the role-mapping conditions.

## How do I change user resource roles when job assignments change?

When job assignments change, you can update the resource role assigned to the employee. Updating a resource role involves these steps:

- Assigning the user a new resource role that corresponds to the new job assignment, for example, Sales Manager.

- Setting an end date for the old resource role, for example, Salesperson.

If the employee's new role also involves a change in the user's resource organization, for example, if the user is promoted to a management role from a non-management role, you must also change the user's organization membership.

You can make changes to role assignments using either the resource import management functionality or using the Sales UI. Although importing changes takes care of many tasks that you have to perform manually in the UI, if you're updating resource role information for an individual user, then using the UI can be more efficient.

These steps describe how to update role information in the UI for a user who's promoted from a sales representative role to a sales manager role.

1. Sign in to the application as the sales administrator or as a setup user.
2. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
3. Search for and select the user who's being promoted. The Edit User page for the user opens.
4. In the Resource Information region, do the following:
    a. In the **Resource Role** field, add the new resource role for the user, for example, **Sales Manager**.
    b. In the **Reporting Manager** field, update the user's manager.
    c. In the **Organization** field, specify the user's resource organization.

       You must create a resource organization for every manager in your Sales organization. If you haven't created a resource organization for the new manager, then you can create one by clicking the **Create** link from the end of the Organization list. The **Create Organization** dialog box is displayed allowing you to enter a new organization name.
    d. To automatically provision any roles provided by the new resource role you just assigned the user, click the **Autoprovision Roles** button in the Resource Information section.
    e. Click **Save and Close**.
5. Set an end date for the user's old resource role using these steps:
    a. Form the Navigator menu, select **Directory** > **Resource Directory**.
    b. In the Tasks area of the Resource Directory page, select **View Resources**.
    c. On the View Resources page, search for and select the user.

       The Resource page for the user opens.

       Note that the user is assigned the new resource organization you previously created.
    d. Click the Roles tab, and 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.
    e. Click **Save and Close**.

> **Note:** When you promote a user from one management position to another, for example, from a Sales Manager role to a Sales VP role, then the resource hierarchy is maintained provided that the promoted user's resource organization doesn't change. So any users who reported to the Sales Manager continue to report to the same individual when that individual is promoted to the Sales VP role. If the promoted user's resource organization does change upon the promotion, the user's reports must be reassigned to a new manager.

For information about changing role assignments using the resource import management functionality, see the topic about importing resource data in the Understanding Import and Export Management for Sales and Fusion Service guide.

*Related Topics*

- How do I import resource data?
- How do I make an employee a sales resource?

# How can I change the name of the top resource organization and other resource organizations?

You can change the name of the top resource organization or any other resource organization by editing the name using the Manage Internal Resource Organizations task.

1. In Setup and Maintenance, go to the **Manage Internal Resource Organizations** task:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Internal Resource Organizations
2. You can search for the organization by name, or select **Sales** as the **Usage** for your search.
3. Edit the organization name and save your changes.

# How are the records of a terminated employee reassigned?

After you terminate an employee in the application, the assignment process automatically excludes the terminated user when it runs again. But you must manually handle other reassignments, for example, replacing the terminated user with another user on the territory team.

For specific types of records, such as lead records or opportunity records, you can also use the Mass Transfer tool to transfer records from a terminated resource to another resource.

*Related Topics*

- Transfer Records Between Users
- About Transferring Records Between Users

# How do I change user resource roles when job assignments change?

When job assignments change, you can update the resource role assigned to the employee. Updating a resource role involves these steps:

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

If the employee's new role also involves a change in the user's resource organization, for example, if the user is promoted to a management role from a non-management role, you must also change the user's organization membership.

You can make changes to role assignments using either the resource import management functionality or using the Sales UI. Although importing changes takes care of many tasks that you have to perform manually in the UI, if you're updating resource role information for an individual user, then using the UI can be more efficient.

These steps describe how to update role information in the UI for a user who's promoted from a sales representative role to a sales manager role.

1. Sign in to the application as the sales administrator or as a setup user.
2. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
3. Search for and select the user who's being promoted. The Edit User page for the user opens.
4. In the Resource Information region, do the following:
    a. In the **Resource Role** field, add the new resource role for the user, for example, **Sales Manager**.
    b. In the **Reporting Manager** field, update the user's manager.
    c. In the **Organization** field, specify the user's resource organization.

       You must create a resource organization for every manager in your Sales organization. If you haven't created a resource organization for the new manager, then you can create one by clicking the **Create** link from the end of the Organization list. The **Create Organization** dialog box is displayed allowing you to enter a new organization name.
    d. To automatically provision any roles provided by the new resource role you just assigned the user, click the **Autoprovision Roles** button in the Resource Information section.
    e. Click **Save and Close**.
5. Set an end date for the user's old resource role using these steps:
    a. Form the Navigator menu, select **Directory** > **Resource Directory**.
    b. In the Tasks area of the Resource Directory page, select **View Resources**.
    c. On the View Resources page, search for and select the user.

       The Resource page for the user opens.

       Note that the user is assigned the new resource organization you previously created.
    d. Click the Roles tab, and 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.

e. Click **Save and Close**.

**Note:** When you promote a user from one management position to another, for example, from a Sales Manager role to a Sales VP role, then the resource hierarchy is maintained provided that the promoted user's resource organization doesn't change. So any users who reported to the Sales Manager continue to report to the same individual when that individual is promoted to the Sales VP role. If the promoted user's resource organization does change upon the promotion, the user's reports must be reassigned to a new manager.

For information about changing role assignments using the resource import management functionality, see the topic about importing resource data in the Understanding Import and Export Management for Sales and Fusion Service guide.

*Related Topics*

- How do I import resource data?
- How do I make an employee a sales resource?

# Can I reactivate a terminated employee record?

Yes. Once you specify an end date for a resource, you can't reverse it in the application. But the former employee's record remains in the application so you can again identify that person as a resource if the person is rehired.

After identifying the person, you must assign roles and an organization again.

# How can I notify users of their user names and passwords?

You can run the Send User Name and Password Email Notifications process in the Scheduled Processes work area. For users for whom you haven't so far requested an email, this process sends out user names and reset-password links.

The email goes to the work email of the user or the user's line manager. You can send the user name and password once only to any user. A notification template for this event must exist and be enabled.