Oracle Sales Cloud
Securing Sales

Release 13 (update 18C)
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>i</td>
</tr>
<tr>
<td>1 About This Guide</td>
<td>1</td>
</tr>
<tr>
<td>Audience and Scope</td>
<td>1</td>
</tr>
<tr>
<td>Related Guides</td>
<td>1</td>
</tr>
<tr>
<td>2 Authentication</td>
<td>3</td>
</tr>
<tr>
<td>Authentication and Identity Management</td>
<td>3</td>
</tr>
<tr>
<td>Single Sign-On Authentication</td>
<td>3</td>
</tr>
<tr>
<td>3 Authorization with Role-Based Access Control</td>
<td>5</td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td>5</td>
</tr>
<tr>
<td>Predefined Sales Roles</td>
<td>5</td>
</tr>
<tr>
<td>Roles for Workflow Administration Access</td>
<td>6</td>
</tr>
<tr>
<td>Role Types</td>
<td>7</td>
</tr>
<tr>
<td>About Role Hierarchies and Inheritance</td>
<td>8</td>
</tr>
<tr>
<td>Security Policies</td>
<td>10</td>
</tr>
<tr>
<td>Security Configuration: Points to Consider</td>
<td>11</td>
</tr>
<tr>
<td>Reviewing Predefined Roles</td>
<td>12</td>
</tr>
<tr>
<td>Oracle Cloud Applications Security Console</td>
<td>13</td>
</tr>
<tr>
<td>4 Data Sharing Mechanisms and Object Visibility</td>
<td>15</td>
</tr>
<tr>
<td>Data Sharing Mechanisms</td>
<td>15</td>
</tr>
<tr>
<td>How Users Gain Access to Opportunities</td>
<td>15</td>
</tr>
<tr>
<td>How Users Gain Access to Leads</td>
<td>18</td>
</tr>
<tr>
<td>Multiple Business Units and Data Access</td>
<td>18</td>
</tr>
</tbody>
</table>
5 Setting Up Applications Security

- Defining Security Synchronization Processes and Preferences: Overview 21
- Importing Users and Roles into Applications Security 21
- Synchronizing User and Role Information 22
- Managing Application Security Preferences 22
- Setting the Default User Name Format 23
- Setting Password Policy 24
- Setting Role Preferences 26
- User Categories 27
- Adding Users to a User Category 28
- Managing User-Name and Password Notifications 29
- Creating a Notification Template 31
- Scheduling the Import User and Role Application Security Data Process 32
- Importing User Login History 33
- Send Pending LDAP Requests 33
- Scheduling the Send Pending LDAP Requests Process: Procedure 34

6 Working with the Bridge for Microsoft Active Directory

- Bridge for Microsoft Active Directory: Explained 37
- Synchronizing Information Between Source and Target Applications: Explained 37
- Mapping Information Between Source and Target Applications for Synchronization: Explained 38
- Using the Bridge for Microsoft Active Directory 40
- FAQs on Working with the Bridge for Microsoft Active Directory 45

7 Sales Cloud Users and Role Provisioning

- About Sales Cloud Users 47
- Methods of Creating Users 49
- Tasks You Accomplish by Creating Users 50
- About Provisioning Job and Abstract Roles to Users 51
- Steps for Setting Up Role Provisioning 55
## 8 Getting Ready to Create Sales Users

- What You Must Do Before Creating Sales Users
- Creating a Resource Organization
- Designating an Organization as the Top of the Sales Hierarchy
- Creating Additional Resource Roles
- Creating Rules to Automatically Provision Job Roles to Sales Users
- Automatic and Manual Role Provisioning
- Enabling Validation of Work Email Values
- Provisioning Roles for Testing
- FAQs for Preparing for Application Users

## 9 Creating Sales Users

- User Setup Options
- Creating Application Users
- Creating Sales Restricted Users

## 10 Managing Sales Users

- Managing Users: Overview
- Resetting Passwords for Users
- Changing a User's E-Mail Address
- Changing User Names
- Changing User Resource Roles When Job Assignments Change
- Terminating User Accounts
- FAQs for Terminating Users
- Impersonation and Proxy Users

## 11 Reporting on Application Users and Roles

- User and Role Access Audit Report
- User Role Membership Report
- User Password Changes Audit Report
- Inactive Users Report
- User History Report
# Oracle Sales Cloud

## Securing Sales

### 12 Using the Security Console to Review and Analyze Roles

- Reviewing Roles on the Security Console: Overview
- Graphical and Tabular Role Visualizations
- Reviewing Role Hierarchies
- Simulating Navigator Menus in the Security Console
- Reviewing Role Assignments
- Comparing Roles
- Role Analytics
- Security Console Analytics for Database Resources

### 13 Creating Job, Abstract, and Duty Roles

- Security Configuration: Overview
- Copying Sales Roles: Points to Consider
- Copying Job or Abstract Roles
- Editing Job or Abstract Roles
- Creating Job or Abstract Roles
- Copying and Editing Duty Roles
- Editing Data Security Policies on the Security Console

### 14 Reviewing and Configuring Data Security

- Configuring Data Security: Overview
- Reviewing Data Access for a Role and Object
- Editing the Data Access Permissions for a Custom Role and an Object
- Extending Access to Additional Objects for a Custom Role
- Managing Database Resources

### 15 Security and Reporting

- Security for Sales Cloud Analytics and Reports
- Permissions for Catalog Objects
- Transaction Analysis Duty Roles
- Business Intelligence Roles
- Configuring Security for Oracle Transactional Business Intelligence: Explained
- Viewing Reporting Roles
- FAQs for Security and Reporting
<table>
<thead>
<tr>
<th>Chapter Number</th>
<th>Section Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td><strong>Security and Personally Identifiable Information</strong></td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>Security and Personally Identifiable Information: Overview</td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>Protecting Personally Identifiable Information</td>
<td>127</td>
</tr>
<tr>
<td>17</td>
<td><strong>Role Optimization</strong></td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>Role Optimizer Overview</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>Role Optimization Report</td>
<td>131</td>
</tr>
<tr>
<td>18</td>
<td><strong>Advanced Data Security</strong></td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Advanced Data Security</td>
<td>133</td>
</tr>
</tbody>
</table>
Preface

This preface introduces information sources that can help you use the application.

Using Oracle Applications

Using Applications Help

Use help icons to access help in the application. 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. Not all pages have help icons. You can also access Oracle Applications Help.

Watch: This video tutorial shows you how to find help and use help features.

You can also read Using Applications Help.

Additional Resources

- **Community**: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.

- **Guides and Videos**: Go to the Oracle Help Center to find guides and videos.

- **Training**: Take courses on Oracle Cloud from Oracle University.

Conventions

The following table explains the text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than symbol separates elements in a navigation path.</td>
</tr>
</tbody>
</table>

Documentation Accessibility

For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website.

Videos included in this guide are provided as a media alternative for text-based help topics also available in this guide.
Contacting Oracle

Access to Oracle Support
Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

Comments and Suggestions
Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
Chapter 1

About This Guide

Audience and Scope

This guide is intended for anyone who is involved in implementing and administering security. Some of the tasks described in this guide are performed only or mainly during implementation of the sales application. Most, however, can be performed at any time and as new requirements emerge. This guide provides information about:

- How role-based access control is implemented
- How users gain visibility to object data.
- How to create and manage application users, and how to provision users with roles to provide them with access to application functions and data.
- How to set up, manage, and use the Security Console.
- How to create security artifacts, such as security policies and roles.

During implementation, you perform security-related tasks from a functional area task list or implementation project. Once the implementation is complete, you can perform most security-related tasks on the Security Console. Any exceptions are identified in relevant topics. For example, you create users in the Manage Users work area, not on the Security Console.

Related Guides

The following table lists related guides used during the implementation and administration of Oracle Sales Cloud.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Sales Cloud Getting Started with Your Sales Implementation</td>
<td>Describes how to set up a sales automation solution in Oracle Sales Cloud using a case study to describe concepts and procedures.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Implementing Sales</td>
<td>Describes how to configure and set up Sales.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Extending Sales</td>
<td>Describes how to use tools to configure and extend Oracle Sales Cloud.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Understanding File-Based Data Import and Export</td>
<td>Describes how to import object data into Oracle Sales Cloud.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Security Reference</td>
<td>Provides a reference to roles, role hierarchies, privileges, and policies as delivered for the Sales offering.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Creating and Administering Analytics for Sales</td>
<td>Explains how to view and work with analytics and reports.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Implementing Customer Data Management</td>
<td>Describes how to get started with the implementation of Customer Data Management capabilities such as duplicate identification, duplicate resolution, address validation, and data enrichment.</td>
</tr>
</tbody>
</table>

Oracle Sales Cloud
Securing Sales
Related Topics

- Oracle Help Center
2 Authentication

Authentication and Identity Management

This topic describes the authentication and identity management services provided by Oracle for Cloud Applications.

Standard Authentication for Cloud Applications

Authentication, the process of verifying that a user is who they claim to be, is applied to all users, automated agents, or Web services that access an Oracle Cloud application. User credentials are checked at login and access is then granted or denied. In the standard method of authentication provided for Oracle Cloud environments, authentication providers validate user and application access based on a user name-password combination. Authentication providers also make user identity information available to other Cloud components when needed.

Identity Store

The Oracle Cloud authentication providers access the LDAP identity store, which is a logical repository of enterprise user identity data. Your LDAP directory stores definitions of LDAP user accounts.

In general, changes you make to user accounts are automatically synchronized between your sales application and your LDAP directory server. However, you must also run processes on a daily basis to manage information exchange between your application and your LDAP directory server. For information, see the chapter about setting up application security.

Single Sign-On Authentication

Single Sign-On authentication, which enables users to sign in once but access multiple applications, is optionally available for user authentication.

If your enterprise has moved from a traditional on-premises environment to an Oracle cloud service, you might want to use your existing identity management solution for authenticating your employees in the cloud service, and might also want to provide a Single Sign-On experience. Implementing federated Single Sign-On allows you to provide users with Single Sign-On access to applications and systems located across organizational boundaries. For additional information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at https://support.oracle.com.

Note: Single Sign-On authentication is available on all platforms used to access the application, including Oracle Mobile platforms, and is also available for Web services.
3 Authorization with Role-Based Access Control

Role-Based Access Control

When you receive your Oracle Cloud application, access to its functionality and data is secured using the industry-standard framework for authorization, role-based access control. You must implement the role-based access controls provided by Oracle so that users have appropriate access to sales data and functions.

In a role-based access control model, users are assigned roles, and roles are assigned access privileges to protected resources. The relationship between users, roles, and privileges is shown in the following figure.

In the sales application, users gain access to application data and functions when you assign them roles, which correspond to the job functions in your organization.

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

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

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

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

Related Topics

- Provisioning Job and Abstract Roles to Users: Explained
Predefined Sales Roles

Oracle provides many predefined job and abstract roles for the sales application. The following are the main predefined job roles for sales users:

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

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

- Employee
- Resource

These predefined roles are part of the Oracle security reference implementation for the sales application. The security reference implementation is a predefined set of security definitions that you can use as supplied.
Roles for Workflow Administration Access

Predefined roles provide access to workflow administration functionality. Users with these roles can, for example, set up approval rules and manage submitted approval tasks. This table identifies the predefined Oracle Business Process Management (BPM) role for sales workflow administration access, and the predefined job roles that inherit it. It also shows the BPM role that provides workflow administration access for all product families. You can assign a predefined BPM role to a custom job role, if required.

<table>
<thead>
<tr>
<th>Product Family</th>
<th>Role Name and Code</th>
<th>Inherited by Job Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>BPM Workflow Customer Relationship Management Administrator</td>
<td>Corporate Marketing Manager (ORA_MKT_CORPORATE_MARKETING_MANAGER_JOB)</td>
</tr>
<tr>
<td></td>
<td>BPMWorkflowCRMAAdmin</td>
<td>Customer Relationship Management Application Administrator (ORA_ZCA_CUSTOMER_RELATIONSHIP_MANAGEMENT_APPLICATION_ADMINISTRATOR_JOB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Analyst (ORA_MKT_MARKETING_ANALYST_JOB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Manager (ORA_MKT_MARKETING_MANAGER_JOB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Operations Manager (ORA_MKT_MARKETING_OPERATIONS_MANAGER_JOB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing VP (ORA_MKT_MARKETING_VP_JOB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sales Lead Qualifier (ORA_MKL_SALES_LEAD_QUALIFIER_JOB)</td>
</tr>
<tr>
<td>All</td>
<td>BPM Workflow All Domains Administrator Role</td>
<td>This role isn’t assigned to any predefined job role, but you can add it to custom job roles.</td>
</tr>
<tr>
<td></td>
<td>BPMWorkflowAllDomainsAdmin</td>
<td></td>
</tr>
</tbody>
</table>

Role Types

This topic describes the roles provided by your sales application and explains how they work together to provide users with permissions to application resources. The following types of roles are provided:

- Job roles
- Abstract roles
- Duty roles
The permissions each role provides are described in security reference manuals available on http://docs.oracle.com.

Job Roles

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

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

Abstract Roles

Abstract roles represent a worker’s functions in the enterprise independently of the job they do. The following are examples of abstract roles used in the sales application:

- Employee
- Resource

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

Duty Roles

Job and abstract roles permit users to carry out actions by virtue of the duty roles they include. Each predefined duty role consists of a logical grouping of privileges that represents the individual duties that users perform as part of their job. Duty roles are composed of security policies which grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on.

For example, the Sales Manager job role inherits the Sales Lead Follow Up duty and the Sales Forecasting Management duty. The Sales Lead Follow Up duty makes it possible for managers to work with leads. The Sales Forecasting Management duty enables the management of sales forecasts. Job roles and abstract roles can inherit duty roles either directly or indirectly.

You can create duty roles and can include predefined and custom duty roles in custom job and abstract roles. You don’t assign duty roles directly to users.

About Role Hierarchies and Inheritance

This topic describes how users inherit roles and privileges and outlines the role hierarchy, in which each role can be linked to other roles in a parent-child format. As illustrated in the following figure, users are assigned job and abstract roles, which
inherit duty roles and their associated privileges. Duty roles in turn can inherit privileges from subordinate duty roles. You can explore the complete structure of a job or abstract role on the Security Console.

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

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

This example shows how roles and privileges are inherited for a user, Tom Green, assigned the Sales Manager job role. The following figure shows a few representative duty roles.

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

- The Sales Manager job role inherits duty roles including the Sales Party Management duty role and the Opportunity Sales Manager duty role.
- Duty roles inherit other duty roles. For example, the Sales Party Management duty inherits the Sales Party Review duty and the Trading Community Import Batch Management duty, as well as many privileges.
- The duty roles can be associated with functional security policies and data security policies. For example, the inherited Sales Party Review duty includes security policies that specify which application pages sales managers can access to export assets.
Security Policies

Duty roles are associated with two types of security policies: function security policies and data security policies. Security policies define the privileges provided by the duty role to access specific application resources. This topic describes both types of security policy.

-note: The privileges provided by each duty role are described in the security reference manuals available on http://docs.oracle.com.

Function Security Policies

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

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

Some user interfaces aren’t subject to data security, so some function security privileges have no equivalent data security policy.

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

Data Security Policies

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

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

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

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

Policy Store

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

If the predefined security reference implementation doesn’t fully represent your enterprise, then you can make changes. For example, the predefined Sales Representative job role includes sales forecasting privileges. If some business groups in your organization have the sales managers do forecasting, not the sales representatives, then you can create a sales representative role without those privileges.

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

You can identify predefined roles easily by their role codes, which all have the prefix ORA_. For example, the role code of the Sales Representative application job role is ORA_ZBS_SALES_REPRESENTATIVE_JOB.

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

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

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

Predefined Roles with Missing Privileges
If the privileges for a job aren’t defined in the security reference implementation, then you can create your own duty roles. The typical implementation doesn’t use custom duty roles.

Reviewing Predefined Roles
This topic describes the ways in which you can access information about predefined roles. This information can help you to identify which users need each role and whether to make any changes before provisioning roles.

Security Console
On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.
- Identify the function security privileges and data security policies granted to a role.
• Compare roles to identify differences.

💡 **Tip:** The role codes of all predefined roles have the prefix ORA_.

### Reports

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

### Security Reference Manuals

Two manuals describe the security reference implementation for Oracle Sales Cloud users:

- The Oracle Applications Cloud Security Reference for Common Features includes descriptions of all predefined security data that’s common to Oracle Fusion Applications.
- The Oracle Sales Cloud Security Reference includes descriptions of all predefined security data for Oracle Sales Cloud.

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

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

You can access the security reference manuals on cloud.oracle.com. From the menu select Resources > Documentation > Applications. Select Sales Cloud, then Books.

### Oracle Cloud Applications Security Console

The Security Console is an easy-to-use administrative work area where you perform most security-management tasks. This topic introduces the Security Console and describes how to access it.

### Security Console Functions

Use the Security Console to:

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

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

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

Note: Oracle Sales Cloud does not use certificate functionality.

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

Accessing the Security Console

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

• Manage Job Roles
• Manage Duties
• Manage Data Security Policies
4 Data Sharing Mechanisms and Object Visibility

Data Sharing Mechanisms

This chapter describes how users gain visibility to various objects used in the sales application. The conditions specified in data security policies control visibility to record-level data associated with a schema object, such as an opportunity. Conditions can use the following components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

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

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

How Users Gain Access to Opportunities

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

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

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

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

- An opportunity owner gets full access to the opportunity, which includes the ability to edit as well as add and remove team members.
- Owners and members of territories or of ancestor territories assigned to the account of the opportunity get read-only access to the opportunity and are not added to the opportunity sales team.
Owners and members of territories assigned to the opportunity product lines are added as a distinct list of territories to the opportunity sales team. Owners and members of these territories get full access to the opportunity. Depending on a profile option, either only the owner or all the members of the territory are added as resources to the opportunity sales team. Regardless of the access level for these members as a resource on the opportunity team, they always have full access.

Owners and members of ancestor territories of the territory assigned to the opportunity do not get added to the opportunity sales team but they always get full access.

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

- Named agents in the diagram (A, B, and C) can access the opportunity.
- Unnamed agents (highlighted in yellow) cannot access the opportunity.
- Sales managers can access the opportunity because a salesperson in their management chain has access.
This figure shows who in a sales hierarchy can access an opportunity.

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

Note: Access using accounts is not shown in this figure.

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

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

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

How Users Gain Access to Leads
This topic explains how the security reference implementation provided by Oracle determines who can access lead information in your sales organization.

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

You can access a lead if:

• You are the lead owner.

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

• You are a member of the lead sales team.

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

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

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

Multiple Business Units and Data Access
This topic describes how implementing multiple business unit functionality affects access to object transactional data.

A business unit (BU) is a unit of an enterprise that performs one or more business functions, such as Sales or Marketing. A business unit primarily provides a means of separating or sharing setup data and controlling transactional data access within an enterprise. By default, an enterprise structure is created as a single business unit to which all users belong. However, you can create additional business units if required.

Users are associated with a business unit through their resource organization membership. Resource organizations are mapped to one or more business units. When a sales user is created, the user is assigned to a resource organization, and thereby gains access to each business unit that is mapped to the resource organization. For example, users can access
relevant transactional data associated with their primary business unit, but might also have access to relevant transactional data in other business units through their resource organization.

Note: When you create a user in the sales application, you specify a business unit for the user. However, only the BUs associated with the user’s resource organization are relevant in determining the business units a user can access. If a business unit is not specified for a resource organization, the default business unit is used.

Within the sales application, the following business objects support the use of multiple business units:

- Contracts
- Leads
- Opportunities
- Resource Organizations
- Territories

When you create an object that supports multiple business units, such as an opportunity, you specify the business unit to associate with the object.

Object Access in a Single Business Unit Environment (Default)

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

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

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

<table>
<thead>
<tr>
<th>Type of Object Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territory membership</td>
<td>You gain access to an object if:</td>
</tr>
<tr>
<td></td>
<td>o You are the owner or member of the territory that is assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>o You are the owner or member of an ancestor territory of the territory assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>o Your direct or indirect report in the resource hierarchy is the owner or a member of the territory assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>o Your direct or indirect report in the resource hierarchy is the owner or member of an ancestor territory of the territory assigned to the object.</td>
</tr>
<tr>
<td>Team membership</td>
<td>You gain access to an object if:</td>
</tr>
<tr>
<td></td>
<td>o You are a member of the sales team assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>o Your direct or indirect report in the resource hierarchy is a member of the sales team assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>o You are a member of the partner team assigned to the object.</td>
</tr>
</tbody>
</table>
Object Access in a Multiple Business Unit Environment

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

- Sales administrators can access transactional data for all objects that are associated with the business unit or units to which the administrators are assigned.

- Sales users access to transactional data for an object is the same in multiple business unit environments and single business unit environments. That is, sales users can access object data across business unit boundaries provided that they have valid access to the object by means of territory or team membership, through the resource hierarchy, or by being granted full access to the object.

Business unit assignment can, however, indirectly affect a user’s access to object transactional data. In a multiple business unit environment, business units are available as territory dimensions and can be included as part of the territory coverage definition for the assignment of transactions. A sales user gains access to object data through territory membership. If business unit is specified as a territory dimension, then the user’s access to data is limited to objects which, when they were created, were assigned to the same business unit that is assigned to the user’s territory team.
Defining Security Synchronization Processes and Preferences: Overview

During implementation, the initial user, or a setup user with the IT Security Manager job role, prepares the application security environment by performing a number of tasks. The security setup tasks, described in this chapter, include the following:

- Manage Applications Security Preferences
  This task opens the Administration tab of the Security Console. Select the appropriate tab of the Security Console to set enterprise-wide preferences that affect users, roles, and notifications to application users.

- Import Users and Roles into Application Security
  This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables.

- Import User Login History
  This task runs a process that imports the history of user access to Oracle Fusion Applications.

- Run User and Roles Synchronization Process
  This task runs a process that copies data from the LDAP directory to Oracle Fusion Applications Security tables.

In the Setup and Maintenance work area, security setup tasks are located in the Users and Security functional area of the Sales offering.

Importing Users and Roles into Applications Security

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

Running the Import User and Role Application Security Data Process

Sign in as a setup user and follow these steps:

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

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

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

Chapter 5
Setting Up Applications Security

Note: It's recommended that you schedule this process to run daily.

Related Topics
• Accessing Tasks to Update Existing Setup Data: Procedure

Synchronizing User and Role Information

You run the process Retrieve Latest LDAP Changes once during implementation. This process copies data from the LDAP directory to the Oracle Fusion Applications Security tables. Thereafter, the data is synchronized automatically. To run this process, perform the task Run User and Roles Synchronization Process as described in this topic.

Running the Retrieve Latest LDAP Changes Process

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

Related Topics
• Accessing Tasks to Update Existing Setup Data: Procedure

Managing Application Security Preferences

During implementation, a number of options are available on the Security Console for controlling the default functionality of tasks such as working with roles or certificates. Some of these options can be overridden. However, it is recommended that you set these options before you start to create application users or configure your security environment.

To configure these security preferences, the initial user, or a setup user with the IT Security Manager job role, performs the task Manage Applications Security Preferences. This task opens the Administration tab of the Security Console from where you can do the following:
• On the General subtab of the Security Console Administration tab, you:
   o Specify for how long certificates remain valid by default.

Note: Oracle Sales Cloud does not use certificate functionality.
• Specify how often a warning appears to remind Security Console users to import latest user and role information.
• On the Roles subtab of the Security Console Administration tab, you:
  o Specify default prefix and suffix values for copied roles.
  o Specify a limit to the number of nodes that can appear in graphical representations of roles on the Roles tab of the Security Console.
  o Specify whether hierarchies on the Roles tab appear in graphical or tabular format by default.

• On the Bridge for Active Directory subtab of the Security Console Administration tab, you configure the bridge for Microsoft Active Directory.

• On the User Categories tab of the Security Console, you:
  o Create user categories and add users to a category.
  o Specify the default format of user names for the user category.
  o Manage the password policy for a user category.
  o Manage the notification of user and password events to users in a selected user category.
  o Create notification templates for a user category.

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

### Setting the Default User Name Format

During implementation, you specify the default format of user names for the default user category. The default format you select is used to automatically generate a user name for a user if you don’t explicitly specify the user name when you create the user. This topic describes how to specify the default format of user names and the formats that are available.

### Specifying the Format of User Names

Perform the steps in the following procedure to select the default format for user names:

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

   The Administration page of the Security Console opens. (You can also navigate directly to the Security Console at any time by clicking Security Console from the Navigator.)

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

   The following table describes the available user name formats.
### Format Name

<table>
<thead>
<tr>
<th>Format Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>The work email (or party email, for party users) is the user name. For example, the user name for <a href="mailto:john.smith@example.com">john.smith@example.com</a> is <a href="mailto:john.smith@example.com">john.smith@example.com</a>. To make duplicate names unique, a number is added. For example, <a href="mailto:john.smith2@example.com">john.smith2@example.com</a> may be used if <a href="mailto:john.smith@example.com">john.smith@example.com</a> and <a href="mailto:john.smith1@example.com">john.smith1@example.com</a> already exist.</td>
</tr>
<tr>
<td>FirstName.LastName</td>
<td>The user name is the user’s first and last names separated by a single period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user’s middle name or a random character is used. For example, John Smith's user name could be john.frank.smith or john.x.smith.</td>
</tr>
<tr>
<td>FLastName</td>
<td>The user name is the user’s last name prefixed with the initial of the user’s first name. For example, the user name for John Smith is jsmith.</td>
</tr>
<tr>
<td>Person or party number</td>
<td>The person or party number generated by the application is the user name. For example, if John Smith’s party number is 100000000178803, then the user name is 100000000178803. User names generated from party or person numbers can be difficult to remember so it’s recommended that you don’t select this option.</td>
</tr>
</tbody>
</table>

5. Enable or disable the option **Generate system user name when generation rule fails**. This option controls whether a system user name is generated if the user name rule fails. For example, if the default user name format is party number or email but these values aren’t available when the user is created.

   - If the option is enabled, a system user name is generated by applying these options in the following order until a unique user name is defined:
     i. Email
     ii. FirstName.LastName
     iii. If only the last name is available, then a random character is prefixed to the last name.
   - If the option is disabled, then an error is raised if the user name can’t be generated in the selected format.

6. Click **Save and Close**. Any changes take effect immediately.

### Editing User Names

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

**Related Topics**

- Accessing Tasks to Update Existing Setup Data: Procedure

### Setting Password Policy

During implementation, you set the password policy for the default user category. This topic describes the available options. To set the password policy, you perform the Manage Applications Security Preferences task, which opens the Administration
page of the Security Console. Click the User Categories tab and click the name of the default category to open it. Click **Edit** on the Password Policy subtab to edit the policy. You can change the password policy for any user category at any time.

**Password Policy Options**

This table describes the available options for setting password policy.

<table>
<thead>
<tr>
<th>Password-Policy Option</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Before Password Expiration</td>
<td>Specifies the number of days for which a password remains valid. After this period, users must reset their passwords. By default, users whose passwords expire must follow the Forgot Password process.</td>
<td>90</td>
</tr>
<tr>
<td>Days Before Password Expiry Warning</td>
<td>Specifies when a user is notified that a password is about to expire. By default, users are prompted to sign in and change their passwords. This value must be equal to or less than the value of the <strong>Days Before Password Expiration</strong> option.</td>
<td>80</td>
</tr>
<tr>
<td>Note:</td>
<td>This value is 10 for new installations from Release 18B.</td>
<td></td>
</tr>
<tr>
<td>Hours Before Password Reset Token Expiration</td>
<td>When users request a password reset, they’re sent a password-reset link. This option specifies how long a reset-password link remains active. If the link expires before the password is reset, then reset must be requested again. You can enter any value between 1 and 9999.</td>
<td>4</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>Specifies whether passwords must be simple, complex, or very complex. Password validation rules identify passwords that fail the selected complexity test.</td>
<td>Simple</td>
</tr>
<tr>
<td>Disallow last password</td>
<td>Select to ensure that the new password is different from the last password.</td>
<td>No</td>
</tr>
<tr>
<td>Administrator can manually reset password</td>
<td>Passwords can be either generated automatically or reset manually by the IT Security Manager or IT Auditor. Select this option to allow user passwords to be reset manually. All passwords, whether reset manually or generated automatically, must satisfy the current complexity rule.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Note: Users are notified of password events only if appropriate notification templates are enabled for their user categories. The predefined notification templates for these events are Password Expiry Warning Template, Password Expiration Template, and Password Reset Template.

Password Expiry Report

The Password Expiry Report sends the password-expiration-warning and password-expired notifications. You must schedule the Password Expiry Report to run daily. To schedule the report:

1. In the Scheduled Processes work area, click Schedule New Process.
2. In the Schedule Process dialog box, search for and select the Password Expiry Report process.
3. Click OK.
4. In the Process Details dialog box, click Advanced.
5. On the Schedule tab, set Run to Using a schedule.
6. Select a Frequency value. For example, select Daily.
7. Select a start date and time.
8. Click Submit.

Setting Role Preferences

During implementation, you set default role preferences for the enterprise. This topic describes the role preferences and their effects. To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. From there, click the Roles subtab. You can also set role preferences at any time on the Security Console.

Copied-Role Names

To create roles, you’re recommended to copy predefined roles and edit the copied roles. When you copy a predefined role:

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

You specify enterprise prefix and suffix values on the Roles subtab of the Security Console Administration tab. By default:

- Prefix values are blank.
- The role-name suffix is Custom.
- The role-code suffix is _CUSTOM.

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

- Channel Account Manager Custom
- ZPM_CHANNEL_ACCOUNT_MANAGER_JOB_CUSTOM

You can supply prefix values and change the suffix values, as required. If you change these values, then click Save. The changes take effect immediately.
Graph Nodes and Default Views

On the Roles tab of the Security Console, you can display role hierarchies. By default, these hierarchies appear in tabular format. To use graphical format by default, deselect the **Enable default table view** option on the Roles subtab of the Security Console Administration tab.

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

User Categories

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

- Users belong to different organizations within an enterprise and each organization follows a different user management policy.
- Practices related to resetting passwords are not uniform across users.
- Users have different preferences in receiving automated notifications for various tasks they perform in the application.

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

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

Segregate Users into Categories

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

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

Specify Next URL

Specify a URL to redirect your users to a website or an application instead of going back to the Sign In page, whenever they reset their password. For example, a user places a password reset request and receives an email for resetting the password. After the new password is authenticated, the user can be directed to a website or application. If nothing is specified, the user is directed to the Oracle Applications Cloud Sign In page. You can specify only one URL per user category.
Set User Preferences
Select the default format of the User Name, the value that identifies a user when signed in. It is generated automatically in the format you select. For additional information, see the topic Setting the Default User Name Format.

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

Enable Notifications
Notifications are enabled by default, but you can disable them if required. You can also enable or disable notifications separately for each user category. If users belonging to a specific category don’t want to receive any notification, you can disable notifications for all life cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.

Notifications are sent for a set of predefined events. To trigger a notification, you must create a notification template and map it to the required event. Depending on the requirement, you can add or delete a template that is mapped to a particular event. For additional information, see the topic Managing User-Name and Password Notifications.

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

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

Related Topics
• Using REST API to Add Users to a User Category

Adding Users to a User Category
Using the Security Console, you can add existing users to an existing user category or create a new category and add them. When you create new users, they are automatically assigned to the default category. At a later point, you can edit the user account and update the user category. You can assign a user to only one category.

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

You can add users to a user category in three different ways:
• Create a user category and add users to it
• Add users to an existing user category
• Specify the user category for an existing user
Note: You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can’t rename a user category.

Adding Users to a New User Category

To create a user category and add users:

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

Adding Users to an Existing User Category

To add users to an existing user category:

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

Specifying the User Category for an Existing User

To add an existing user to a user category:

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

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

Managing User-Name and Password Notifications

By default, users in all user categories are notified automatically of changes to their user accounts and passwords. These notifications are based on notification templates. Many templates are predefined, and you can create templates for any user category. During implementation, you identify the notifications that you plan to use for each user category and disable
any that aren’t needed. This topic introduces the predefined notification templates and explains how to enable and disable notifications.

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.

<table>
<thead>
<tr>
<th>Notification Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiry Warning Template</td>
<td>Warns the user that a password is expiring soon and provides instructions for resetting the password.</td>
</tr>
<tr>
<td>Password Expiration Template</td>
<td>Notifies the user that a password has expired and provides instructions for resetting the password.</td>
</tr>
<tr>
<td>Forgot User Name Template</td>
<td>Sends the user name to a user who requested the reminder.</td>
</tr>
<tr>
<td>Password Generated Template</td>
<td>Notifies the user that a password has been generated automatically and provides instructions for resetting the password.</td>
</tr>
<tr>
<td>Password Reset Template</td>
<td>Sends a reset-password link to a user who requested a new password.</td>
</tr>
<tr>
<td>Password Reset Confirmation Template</td>
<td>Notifies the user when a password has been reset.</td>
</tr>
<tr>
<td>New Account Template</td>
<td>Notifies a user when a user account is created and provides a reset-password link.</td>
</tr>
<tr>
<td>New Account Manager Template</td>
<td>Notifies the user’s manager when a user account is created.</td>
</tr>
</tbody>
</table>

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. However, you can create templates and disable the predefined versions. Each predefined event can be associated with only one enabled notification template at a time.

Enabling and Disabling Notifications

For any notification to be sent to the users in a user category, notifications in general must be enabled for the user category. Ensure that the Enable notifications option on the User Category: Notifications page is selected. When notifications are enabled, you can disable specific templates. For example, if you disable the New Account Template, then users in the relevant user category aren’t notified when their accounts are created. Other notifications continue to be sent.

To disable a template:

1. On the User Category: Notifications page, click Edit.
2. Click the template name.
3. In the template dialog box, deselect the **Enabled** option.
4. Click **Save and Close**.

Creating a Notification Template

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

Creating a Notification Template

Follow these steps:

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

   This table shows the tokens supported in the message text.

<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>notificationUserName</td>
<td>User name to which notifications are sent</td>
</tr>
<tr>
<td>userEmailAddress</td>
<td>Address to which email notifications are sent</td>
</tr>
<tr>
<td>userLoginId</td>
<td>User name</td>
</tr>
<tr>
<td>firstName</td>
<td>User's first name</td>
</tr>
<tr>
<td>lastName</td>
<td>User's last name</td>
</tr>
<tr>
<td>managerFirstName</td>
<td>Manager's first name</td>
</tr>
<tr>
<td>managerLastName</td>
<td>Manager's last name</td>
</tr>
<tr>
<td>loginURL</td>
<td>URL where the user can sign in</td>
</tr>
</tbody>
</table>
### Setting Up Applications Security

#### Chapter 5

<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>resetURL</td>
<td>URL where the user can reset his or her password</td>
</tr>
<tr>
<td>CRLFX</td>
<td>New line</td>
</tr>
<tr>
<td>SP4</td>
<td>Four spaces</td>
</tr>
</tbody>
</table>

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

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

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

---

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

You must run the **Import User and Role Application Security Data** process to set up and maintain the Security Console. During implementation, you perform the **Import Users and Roles into Application Security** task to run this process. It 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 Oracle Fusion Applications Security tables makes the assisted search feature of the Security Console fast and reliable. After the process runs to completion for the first time, you’re recommended to schedule **Import User and Role Application Security Data** to run daily. This topic describes how to schedule the process.

> **Note:** Whenever you run the process, it copies only those changes that were made since it last ran.

#### Scheduling the Process

Follow these steps to schedule the **Import User and Role Application Security Data** process:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User and Role Application Security Data** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times. The start time should be after any daily run of the **Send Pending LDAP Requests** process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.
Synchronization Process Preferences

On the General subtab of the Security Console Administration tab, you can set the Synchronization Process Preferences option. This option controls how frequently you’re reminded to run the Import User and Role Application Security Data process. By default, the warning appears if the process hasn’t run successfully in the last 6 hours. If you schedule the process to run daily, then you may want to increment this option to a value greater than 24.

Importing User Login History

During implementation, you perform the Import User Login History task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables. This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform Import User Login History for the first time, you’re recommended to schedule it to run daily. In this way, you can ensure that the Inactive Users Report is up to date.

Scheduling the Import User Login History Process

Follow these steps:

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

Related Topics

- Inactive Users Report

Send Pending LDAP Requests

You’re recommended to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to your LDAP directory server. Schedule the process in the Scheduled Processes work area. This topic describes the purpose of Send Pending LDAP Requests.

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

- Requests to create, suspend, and reactivate user accounts.
  - When you create a person record for a worker, a user-account request is generated automatically.
  - When a person has no roles and no current work relationships, a request to suspend the user account is generated automatically.
A request to reactivate a suspended user account is generated automatically if you rehire a terminated worker. The process sends these requests to the LDAP directory unless the automatic creation and management of user accounts are disabled for the enterprise.

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

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

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

**Scheduling the Send Pending LDAP Requests Process: Procedure**

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

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

### Scheduling the Send Pending LDAP Requests Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
3. In the Schedule New Process dialog box, search for and select the **Send Pending LDAP Requests** process.
4. In the Process Details dialog box, set **User Type** to identify the types of users to be processed. Values are **Person**, **Party**, and **All**. You’re recommended to leave **User Type** set to **All**.
5. The **Batch Size** field specifies the number of requests in a single batch. For example, if 400 requests exist and you set **Batch Size** to **25**, then the process creates 16 batches of requests to process in parallel.

   The value **A**, which means that the batch size is calculated automatically, is recommended.
6. Click **Advanced**.
7. On the Schedule tab, set **Run** to **Using a schedule**.
8. In the **Frequency** field, select **Daily**.
9. Enter the start and end dates and times.
10. Click **Submit**.
6 Working with the Bridge for Microsoft Active Directory

Bridge for Microsoft Active Directory: Explained

The bridge for Microsoft Active Directory synchronizes user account information between Oracle Applications Cloud and Microsoft Active Directory. Using the bridge, you can copy user or role details from Oracle Applications Cloud (as the source) to Active Directory (as the target), or the other way around. Depending on the direction in which data synchronization is planned, you can specify one of them as the source and the other one as the target.

Using the Bridge for Microsoft Active Directory

To use the bridge for Active Directory and synchronize information between Oracle Applications Cloud and Active Directory, perform the following steps:

1. Configure the bridge for Active Directory. Set the configuration options on the Administration tab in the Security Console.
2. Map attributes between source and target applications for synchronization.
3. Download and install the bridge for Active Directory.
4. Perform initial synchronization of users.
5. Perform manual or automatic synchronization regularly to maintain consistency of data on the source and target applications.

Prerequisites

Before setting up the bridge between Active Directory and Oracle Applications Cloud, you must:

- Install Java Runtime environment (JRE). The bridge is compatible with JRE versions 6, 7, and 8.
- Install the bridge on a computer that can connect to your Active Directory server.
- Enable Single Sign-On (SSO) between Oracle Applications Cloud and your Active Directory instance.

Related Topics

- Running Bridge for Active Directory with Oracle Applications Cloud as the source
- Running Bridge for Active Directory with Active Directory as the source

Synchronizing Information Between Source and Target Applications: Explained

The bridge for Active Directory synchronizes user account information between Oracle Cloud Applications and Microsoft Active Directory.
After you provide the bridge configuration details, map the user account attributes between Oracle Cloud Applications and Microsoft Active Directory. When the mapping is complete, install and run the bridge for active directory. Initiate the initial synchronization of users between the source and target applications from the bridge application.

During synchronization, the bridge extracts data from the source and target applications, compares the data, and identifies the task that must be performed on the target application for consistency.

When synchronization completes, the bridge performs the required tasks on the target application. Any errors encountered during synchronization are recorded in the log files for review and correction.

After the initial synchronization is complete, you can configure the bridge to synchronize any changes between the source and target at regular intervals or on-demand.

The bridge for active directory can perform:

- Full synchronization
- Incremental synchronization

### Full Synchronization

The bridge starts full synchronization or full reconciliation when any of the following conditions are true:

- The source and target applications are synchronized for the first time.
- The bridge configuration for the active directory has changed.
- The **Run Full Synchronization** button is clicked.

To perform a full synchronization:

1. Click the Bridge for Active Directory tab on the Administration page in the Security Console.
2. Click **User Attribute Mappings**.
3. Expand the On Demand Synchronization section and click **Run Full Synchronization**.

**Note:** To disable full synchronization, click **Cancel Full Synchronization**.

### Incremental Synchronization

The bridge starts incremental synchronization when: any of the following conditions are true:

- The source and target were previously synchronized.
- The bridge configuration for the active directory has not changed.
- The **Run Full Synchronization** button isn’t clicked.

Incremental synchronization can be either on-demand (manually) or at regular intervals (automatically).
Mapping Information Between Source and Target Applications for Synchronization: Explained

After you install and configure the bridge, map the user account attributes between Oracle Cloud Applications and Microsoft Active Directory. Only when the mapping is complete, you can initiate the initial synchronization of users between the source and target applications.

Map the following user attributes:

- User account attributes
- Advanced user account attributes
- Group attributes

Mapping User Attributes

The following attributes of an Oracle Cloud Application user account are mapped to the corresponding attributes of an Active Directory user account:

- **displayName**: Display name of the user account.
- **emails.value**: Primary email associated with the user account.
- **name.familyName**: Last name of the user.
- **name.givenName**: First name of the user.
- **userName**: User name associated with the user account.

During synchronization, the attribute values from the source are copied over to the mapped target attributes.

The following table lists a typical mapping of attributes when Oracle Cloud Application is the source.

<table>
<thead>
<tr>
<th>Oracle Cloud Application as Source</th>
<th>Microsoft Active Directory as Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>emails.value</td>
<td>Mail</td>
</tr>
<tr>
<td>Username</td>
<td>cn</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>name.familyName</td>
<td>sn</td>
</tr>
<tr>
<td>name.givenName</td>
<td>givenName</td>
</tr>
<tr>
<td>Username</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>Username</td>
<td>sAMAccountName</td>
</tr>
</tbody>
</table>
The following table lists a typical mapping of attributes when Microsoft Active Directory is the source.

<table>
<thead>
<tr>
<th>Microsoft Active Directory as Source</th>
<th>Oracle Cloud Applications as Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>emails.value</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>Username</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>givenName</td>
<td>name.givenName</td>
</tr>
<tr>
<td>sn</td>
<td>name. familyName</td>
</tr>
</tbody>
</table>

On the Security Console, click **Administration > Bridge for Active Directory** tab > **User Attribute Mappings**. Click **Add** to add or update the mapping between attributes of the source and target applications.

**Mapping Advanced Attributes**

This is applicable when Active Directory is the source. Use the **Synchronize User Status** option to enable the account status, such as **Disabled**, to propagate to Oracle Cloud Applications.

**Using the Bridge for Microsoft Active Directory**

**Configuring the Bridge for Microsoft Active Directory: Procedure**

Follow this procedure to configure the Bridge for Microsoft Active Directory. Sign in to Oracle Cloud Applications environment as an administrator with the IT Security Manager (**ORA_FND_IT_SECURITY_MANAGER_JOB**) role.

1. Click **Navigator > Security Console**.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click **Configuration**.
4. Expand the Base Configuration section and provide the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Truth</td>
<td>Select the source, such as Oracle Applications Cloud or Active Directory.</td>
</tr>
<tr>
<td>Synchronization Interval (Hours)</td>
<td>Enter the time interval (in hours) that the bridge uses to begin synchronization automatically. The default value is one hour.</td>
</tr>
<tr>
<td>Synchronization Paging Size</td>
<td>Enter the number of accounts that are synchronized in a single operation. The default value is 100 records.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Synchronization Error Threshold | Enter the maximum number of errors that can occur during synchronization. When the limit is reached, synchronization fails and stops. By default, synchronization stops after 50 errors have occurred.
Scheduler | Specify whether you want to automatically schedule synchronizations. If enabled, the synchronizations will run automatically as per the specified schedule and interval.
Role Integration | Specify whether you want to use role integration. It is applicable when Active Directory is the source.
Reset APPID Password | Enter a new password. During synchronization, this password is used by the bridge to connect to Oracle Cloud Applications.

5. Expand the Logging Configuration section and provide the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Enter the name of the log file. This file is created in the Active Directory folder on the computer where the Active Directory bridge is installed. The default value is ad_fa_synch.log</td>
</tr>
<tr>
<td>Log Level</td>
<td>Specify the level at which messages must be logged during synchronization. The default level is set to Information.</td>
</tr>
<tr>
<td>Maximum Log Size</td>
<td>Specify the maximum size of the log file. The default value is 4 GB. When the maximum size is reached, a new log file is created.</td>
</tr>
</tbody>
</table>

6. Expand the Active Directory Configuration section and provide the following details. The bridge uses this information to connect to the Active Directory server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host address of the Active Directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port of the Active Directory server. The default non-SSL port is 389.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select this option for secure communication with the Active Directory server. When you select this option, the default port changes to 636.</td>
</tr>
<tr>
<td>Synchronization Strategy</td>
<td>Select the algorithm that must be used for synchronization. You can select Directory Synchronization or Update Sequence Number. The default value is Directory Synchronization.</td>
</tr>
</tbody>
</table>

**Note:** If you change the sequence number after the initial configuration, the synchronization process resets.

| User Base DN | Enter the distinguished name of the location in your Active Directory where the user accounts are created or retrieved by the bridge. |
Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
---                                    |---                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
Search Base                           | Enter the same value as the User Base DN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
User Search Filter                    | Enter the LDAP query that is used by the bridge to retrieve the user account objects from the Active Directory. For example, (& (objectClass=user)(!(objectClass computer))).                                                                                                                                                                                                                                                                                                                                 |
Group Base DN                         | Enter the distinguished name of the location in your Active Directory from where the bridge fetches the groups.                                                                                                                                                                                                                                                                                                                                                                                                              |
Group Search Filter                   | Enter the LDAP query that is used to fetch roles from your Active Directory server. For example, (objectClass= group).                                                                                                                                                                                                                                                                                                                                                      |
**Note:** This field is applicable only when Active Directory is the source. |
**Note:** This field is applicable only when Active Directory is the source. |

7. Expand the Network Proxy Configuration section and provide the details.

**Note:** Provide these details only when Active Directory is the source, and the bridge uses a proxy to connect to the Active Directory server.

Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
---                                    |---                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
Enable Proxy Settings                  | Select this option to enable communication through a proxy between Oracle Applications Cloud and your Active Directory bridge. Use this option when you need to connect from an isolated network host.                                                                                                                                                                                                                                                                                                                                 |
Host                                  | Enter a host name and address for the proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
Port                                  | Enter a port for the proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
Enable SSL                            | Select this option for secure communication with the proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

8. Expand the Heartbeat section and update the following details.

Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
---                                    |---                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
Heartbeat Interval                     | Enter the time interval, in seconds, at which heartbeat notifications are sent from the bridge to Oracle Applications Cloud to signal that the bridge is active. It is set to 60 seconds by default.                                                                                                                                                                                                                                                                                                                                 |

9. Click **Save** and click **OK**.
Downloading and Installing the Bridge for Active Directory: Procedure

Once you have set the configuration details for the bridge, download the bridge for Active Directory on a computer connected to your network. This computer must connect to both Oracle Cloud Application and your Microsoft Active Directory server instance.

2. On the Administration page, click the Bridge for Active Directory tab.
3. Click Launch.
4. Review the message that appears and click OK.
5. Accept the notification to download the bridge file (adbridge.jnlp).
6. Open the bridge file (adbridge.jnlp) from your Web browser.
7. Enter User name and Password to sign in. You can use your Oracle Applications Cloud credentials to sign in.

Note: You must have the IT Security Manager role (ORA_FND_IT_SECURITY_MANAGER_JOB) to access the bridge.

8. Click OK.
9. Click Run to start the bridge.
10. Enter User name and Password. You can use your Oracle Applications Cloud credentials to sign in.

Note: You must have the IT Security Manager role (ORA_FND_IT_SECURITY_MANAGER_JOB) to access the bridge.

11. Click OK.
12. Open the Bridge for Active Directory. The bridge automatically displays the necessary information configured through the Security Console.
13. Click the Configuration tab.
14. In the Active Directory section, enter the User name and Password for the Active Directory server.
15. In the Oracle Applications Cloud section, enter the Password for the Oracle Applications Cloud host.

Note: The password must match the Reset APPID Password you had provided through the Security Console.

16. You can change the Oracle Cloud Application network settings. Click Network Settings to update the details.
17. Click Save and click Close.

The bridge updates the setup information from Active Directory (attributes, groups) to Oracle Applications Cloud. Use this setup information to perform mapping in the Security Console.

Mapping Attributes and Groups for Synchronization: Procedure

Once you have set the configuration details for the bridge through the Security Console, download the bridge to a computer connected to your network. This computer must connect to both Oracle Applications Cloud and your Microsoft Active Directory server instance.

1. Click Navigator > Security Console.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click User Attribute Mappings.
4. Click Add to update the mapping between source user attributes and target user attributes.
5. Select the source attribute from the Source User Attribute list.
6. Select the target attribute from the Target User Attribute list.
7. Click OK.
8. Repeat steps 4 to 7 to map more attributes.
9. Click Save.
10. Expand the Advanced Attribute Mappings section.
11. Set the Synchronize User Account Status to either enable or disable, to determine whether to synchronize the account or not.
12. Click Save.
13. Click Group Mappings to map active directory groups to Oracle Cloud Application roles.
14. Click Add to add new group to role mapping or select an existing mapping and click the Actions drop-down list.
15. On the Add Role Mapping dialog box, select the Group and the Roles. When a user account is added to or removed from a group in the Active Directory, the corresponding Oracle Cloud Application user account is added to or removed from the mapped role in Oracle Cloud Applications.
16. Click OK.
17. Click Save.

Performing Initial Synchronization: Procedure

Follow these steps to perform the initial synchronization of users:

1. Start the Bridge for Active Directory.
2. Sign in to bridge using your Oracle Cloud Applications login credentials.
3. Click the Synchronization tab.
4. Click Run Now.
5. Click See Log Files to view the log files for any errors.
6. Click Close.

Performing Manual and Automatic Synchronization: Procedures

In the initial synchronization, data is copied from the source application to the target application. After the initial synchronization is complete, you can configure the bridge to synchronize any changes between the source and target applications, either on-demand (manually) or at regular intervals (automatically).

Manual Synchronization

Perform manual synchronization whenever you want to synchronize the source and target applications after the initial synchronization. To manually synchronize data, perform the following steps on the bridge:

1. Navigate to the Security Console and click the Active Directory tab.
2. Click the Synchronization tab and click Run Now.

Automatic Synchronization

You can configure the bridge to perform synchronization periodically as a Microsoft Windows service. Perform the following steps to configure automatic synchronization:

1. Start the bridge.
2. Click **Service Installation**.
3. Enter the user name and password of the account that is used to run the service. The account must have administrative privileges.
4. Click **Install Windows Service**.

On successful installation, the bridge is registered as a service with the name Bridge for Active Directory.

### Specifying the Synchronization Interval

Once the bridge is set up to run as a Windows Service, it periodically performs synchronization. The synchronization interval is specified in the Security Console and must be specified before the bridge is downloaded.

1. Select **Navigator > Security Console**.
2. Click the Administration tab.
3. Click the **Bridge for Active Directory** link.
4. Go to the Configuration tab and specify the Synchronization Interval (in hours).

### FAQs on Working with the Bridge for Microsoft Active Directory

**Can the bridge support other LDAP directories?**

No, the bridge can only be used for synchronization between Oracle Cloud Applications and Microsoft Active Directory.

**How often is information synchronized?**

Using the Microsoft Windows service, you can configure the bridge to perform synchronization periodically. The minimum interval between two synchronizations must be one hour.

**What types of Active Directory objects can be synchronized?**

You can synchronize Active Directory users and groups.

Use the following synchronization options:

- Synchronize users with Oracle Applications Cloud user accounts.
- Synchronize groups with Oracle Applications Cloud roles.

You can synchronize users when the source is either Oracle Applications Cloud or Active Directory. However, you can synchronize groups when the source is only Active Directory.

**What attributes can I synchronize?**

You can synchronize the following predefined attributes in Oracle Applications Cloud with any Active Directory attributes:
### Attribute Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayName</td>
<td>Display name of the user account.</td>
</tr>
<tr>
<td>emails.value</td>
<td>Primary email address associated with the user account.</td>
</tr>
<tr>
<td>name.familyName</td>
<td>Last name of the user.</td>
</tr>
<tr>
<td>name.givenName</td>
<td>First name of the user.</td>
</tr>
<tr>
<td>Username</td>
<td>User name (name for signing in) associated with the user.</td>
</tr>
</tbody>
</table>

You can’t change or format an attribute during synchronization.

⚠️ **Note:** You can synchronize only the predefined attributes, not any user-defined attribute.

### How can I view the log files?

To view the log files, click the Synchronization tab on the bridge application and click the **See Log Files** link. Information about each synchronization is recorded in the log files. The path to the log file on a Windows operating system is: %APPDATA%\Oracle\AD Bridge\log.
7 Sales Cloud Users and Role Provisioning

About Sales Cloud Users

After you have signed up with your Oracle cloud service, you receive the user name and password for one initial user. The initial user is provisioned with the job roles and privileges necessary to perform many implementation tasks, including creating other users. 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: The user types outlined are suggestions. The privileges granted to any user are entirely dependent on the assigned job and abstract roles so, for example, you can create a sales user who is also a setup user if you want.

Initial Users

The initial user is configured to perform many security tasks, including the creation of other users, however, the initial user cannot perform all implementation tasks without assigning themselves additional privileges. For example, the initial user can submit scheduled processes but can't monitor their status.

The roles assigned to the initial user are:

- 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 following types of user.

Setup Users

You can create setup users and provision them with the same job roles as the initial user so that they can help to perform all the standard implementation set up tasks for your sales application. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges.

You also need to provision setup users with the following additional roles:

- Sales Analyst job role
  Makes it possible to create Sales Predictor rules.
- Sales Administrator job role
  Permits the setup user to perform the same tasks as a sales administrator, such as set up and administer sales territories and processes.
- Employee abstract role
Provides the ability to run and monitor background processes.

Setup users are not part of the sales organization so are not created as resources in the sales application and are not provisioned with the Resource abstract role. You cannot assign sales work to them and they cannot view sales transaction data or reports. However, setup users do have the privileges to assign themselves additional roles to make those tasks possible. For information about creating setup users, see Getting Started with Your Sales Implementation at http://docs.oracle.com/.

Sales Administrators

Sales administrators, like other sales application users, are created as resources and are provisioned with job and abstract roles on the basis of the resource role they are 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 cannot configure sales application security or perform tasks related to an enterprise setup. Sales administrator users are provisioned with the following roles:

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

To create sales administrators, follow the procedure outlined in the topic Creating Application Users.

Sales Application Users

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

Sales users are provisioned with job and abstract roles according to the resource role they are assigned. The provisioned job roles do not permit sales users to perform implementation tasks, but they can perform a functional setup within the application, depending on their role. Sales application users are provisioned with the following 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 is relevant to their role. In some cases, however, users do not require the ability to create, update or delete that data. You can create sales restricted users, who have extensive privileges to view sales data but limited privileges to change data, by provisioning application users with the following roles:

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

Sales restricted users can:

- View accounts, contacts, leads and opportunities.
• Create and modify reports and analytics.
• Update, create and manage service requests.
• Create, update and delete notes, tasks and activities for the Activity object.
• Edit forecasts.
• Access content in Sales Lightbox.

Creating the following types of users as sales restricted users provides these users with the visibility to 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.

Note: The Essential User license provides a user with a read-only subscription to Oracle Sales Cloud. You must create users who are assigned an Essential User license as sales restricted users.

Related Topics
• Creating Sales Restricted Users
• Creating Application Users: Worked Example

Methods of Creating Users

This topic provides information about the methods available for creating users. Review this information before you create setup and sales application users. You can create users in either of the following 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 to create individual sales application users.

• Import users from a file using the Data Import and Export group of tasks from the Setup and Maintenance work area.

Import users from a file if you have a large number of users to create. To import users, you must understand how user attributes are represented in the application and how to map the attributes in your file to the attributes required by the application. You cannot import setup users because the import process requires you to import sales resources. For additional information about importing users, see the following information at http://docs.oracle.com/:

◦ The chapter about importing users from a file in the guide Getting Started with Your Sales Implementation
◦ The chapter about importing employee resources in the guide Understanding File-Based Data Import and Export

Note: You must use the Manage Users work area, and not the Security Console, for creating individual users. Use the Security Console to perform the user management tasks, such as resetting user passwords and updating user email addresses, described in this guide.
Related Topics

- Creating Application Users: Worked Example

Tasks You Accomplish by Creating Users

When you create users, a number of 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.

<table>
<thead>
<tr>
<th>Task Accomplished</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifies a user when a user account is created and provides sign-in details.</td>
<td>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. The application sends the user notifications only once, either on account creation or later, depending on the setup.</td>
</tr>
<tr>
<td>Automatically provision the job and abstract roles that provide the security settings users require to do their jobs.</td>
<td>Job and abstract roles are provisioned based on the autoprovisioning rules discussed later in this chapter.</td>
</tr>
<tr>
<td>Create rudimentary employee records. Employee records are used only if you are also implementing Oracle HCM Cloud, or if you implement it in the future.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

 просмотреть

Note: These tasks do not apply to setup users because they are not created as resources in the organization.

<table>
<thead>
<tr>
<th>Task Accomplished</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create resources that can be assigned sales work such as leads, opportunities, and tasks.</td>
<td>Setup users aren't resources in your application and so can't be assigned to sales teams or view reports.</td>
</tr>
<tr>
<td>Create the resource reporting hierarchy used for reporting, forecasting, and work assignments.</td>
<td>When you create a resource, you specify a manager for that resource and build a resource reporting hierarchy.</td>
</tr>
<tr>
<td>Task Accomplished</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create resource records that individual users can update with personal information to complete a directory of your organization.</td>
<td>Setup users aren’t resources and so their information doesn’t appear in your sales organization directory.</td>
</tr>
<tr>
<td>Create a hierarchy of resource organizations.</td>
<td>Each resource is assigned to a resource organization, and the application builds a hierarchy of these organizations based on the resource reporting hierarchy. Setup users aren’t resources and so aren’t assigned to resource organizations.</td>
</tr>
</tbody>
</table>

**About the Resource Reporting Hierarchy**

You build a resource reporting hierarchy when you create sales application users by specifying the manager of each user you create. If you are 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 are 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 Sales Cloud, 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 Oracle Sales Cloud, 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**

- Creating Application Users: Worked Example
About Provisioning Job and Abstract Roles to Users

This topic describes how role provisioning is implemented in the sales application.

About Provisioning Roles to Users

Sales users gain access to data and functions through the job and abstract roles they are assigned. Roles are provisioned to users through predefined role provisioning rules, or through provisioning rules you create using the Manage HCM Role Provisioning Rules task from the Setup and Maintenance work area. Each provisioning rule, also known as a role mapping, defines the following:

- The job and abstract roles to provision
- The conditions that must exist for the roles to be provisioned
- Whether or not 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.

**Note:** The resource role should not be confused with job or abstract roles, which provide the user’s security permissions. The resource role merely describes the role the user plays in the organization and provides the job title which appears in the company resource directory for the user.

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 does not matter if you create users manually in the user interface, or import them from a file.

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

1. 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.
2. The role provisioning rules use the resource role and person type values as conditions.
3. 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.

Note: Oracle provides a predefined rule which automatically assigns the Employee abstract role to all active users who are created as employees, including users who are not sales resources, such as setup users. The Contingent Worker abstract role is automatically assigned to active non-employee users, that is, users created as contingent workers.

Resource Roles and Provisioning Rules Provided by Oracle

Oracle provides resource roles and provisioning rules for provisioning the standard sales job roles to users. The following table lists the role provisioning rules that are provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles the rule provisions. With the exception of 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.

Note: The HR Assignment Status condition is not applicable to partner users who are created as external sales users. As a result, the partner provisioning rules specify only one condition, Resource Role.
For each role assigned by the provisioning rules, the Requestable, Self-Requestable, and Autoprovision options are enabled.

**Note:** If you are using Oracle Sales Cloud in a Global Single Instance (GSI) environment, then Oracle does not provide these role-provisioning rules for you. You must create them manually.

<table>
<thead>
<tr>
<th>Provisioning Rule Name</th>
<th>Condition</th>
<th>Job or Abstract Roles Provisioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Account Manager</td>
<td>HR Assignment Status is Active</td>
<td>Channel Account Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Channel Account Manager</td>
<td>Resource</td>
</tr>
<tr>
<td>Channel Sales Manager</td>
<td>HR Assignment Status is Active</td>
<td>Channel Sales Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Channel Sales Manager</td>
<td>Resource</td>
</tr>
<tr>
<td>Channel Operations Manager</td>
<td>HR Assignment Status is Active</td>
<td>Channel Operations Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Channel Operations Manager</td>
<td>Resource</td>
</tr>
<tr>
<td>Chief Executive Officer</td>
<td>HR Assignment Status is Active</td>
<td>Sales VP</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Chief Executive Officer</td>
<td>Resource</td>
</tr>
<tr>
<td>Contract Administrator</td>
<td>HR Assignment Status is Active</td>
<td>Contract Administrator</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Contract Administrator</td>
<td>Resource</td>
</tr>
<tr>
<td>Contract Manager</td>
<td>HR Assignment Status is Active</td>
<td>Contract Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Contract Manager</td>
<td>Resource</td>
</tr>
<tr>
<td>Customer Data Steward</td>
<td>HR Assignment Status is Active</td>
<td>Customer Data Steward</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Customer Data Steward</td>
<td>Resource</td>
</tr>
<tr>
<td>Data Steward Manager</td>
<td>HR Assignment Status is Active</td>
<td>Data Steward Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Data Steward Manager</td>
<td>Resource</td>
</tr>
<tr>
<td>Partner Administrator</td>
<td>Resource Role is Partner Administrator</td>
<td>Partner Administrator</td>
</tr>
<tr>
<td>Partner Sales Manager</td>
<td>Resource Role is Partner Sales Manager</td>
<td>Partner Sales Manager</td>
</tr>
<tr>
<td>Partner Sales Representative</td>
<td>Resource Role is Partner Salesperson</td>
<td>Partner Sales Representative</td>
</tr>
<tr>
<td>Sales Administrator</td>
<td>HR Assignment Status is Active</td>
<td>Sales Administrator</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Sales Administrator</td>
<td>Resource</td>
</tr>
<tr>
<td>Sales Lead Qualifier</td>
<td>HR Assignment Status is Active</td>
<td>Sales Lead Qualifier</td>
</tr>
</tbody>
</table>


### Provisioning Rule Name

<table>
<thead>
<tr>
<th>Provisioning Rule Name</th>
<th>Condition</th>
<th>Job or Abstract Roles Provisioned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Resource Role is Sales Lead Qualifier</strong></td>
<td>Resource</td>
</tr>
<tr>
<td>Sales Manager</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Sales Manager</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Role is Sales Manager</strong></td>
<td>Resource</td>
</tr>
<tr>
<td>Sales Representative</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Sales Representative</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Role is Salesperson</strong></td>
<td>Resource</td>
</tr>
<tr>
<td>Sales Restricted User</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Sales Restricted User</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Role is Sales Restricted User</strong></td>
<td>Resource</td>
</tr>
<tr>
<td>Sales Setup User</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Application Implementation Consultant</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Role is Sales Setup User</strong></td>
<td>IT Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Diagnostics Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sales Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sales Analyst</td>
</tr>
<tr>
<td>Sales Vice President</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Sales VP</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Role is Sales Vice President</strong></td>
<td>Resource</td>
</tr>
<tr>
<td>Contingent Worker</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Contingent Worker</td>
</tr>
<tr>
<td></td>
<td><strong>System Person Type is Contingent Worker</strong></td>
<td></td>
</tr>
<tr>
<td>Employee</td>
<td><strong>HR Assignment Status is Active</strong></td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td><strong>System Person Type is Employee</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Steps for Setting Up Role Provisioning

Before you create setup or 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 are not provided by Oracle, or your organization uses different job titles.
  For example, you must create an Inside Sales Representative resource role if you want to include the Inside Sales
  Representative 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 Creating Additional Resource Roles.

Create Additional Role Provisioning Rules

Role provisioning rules are provided for the most commonly used resource roles included with the application. You must
create rules for all other resource roles you use.

When you are 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
additional provisioning rules, see the topic Creating Rules to Automatically Provision Job Roles to Sales Users.

Related Topics

- Creating Rules to Automatically Provision Job Roles to Sales Users: Worked Example
8 Getting Ready to Create Sales Users

What You Must Do Before Creating Sales Users

When you create sales application users, either in the UI or by importing them from a file, you not only provision the permissions the users need to do their jobs, but you also build the organization chart for your sales organization. This means that you must set up any additional role provisioning rules you require, 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 are 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 have 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 the topic Creating 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 the topic Creating Resource Organizations. 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 the topic Designating a Resource 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.
   Remember that you are not restricted to assigning one job role to a user. For example, you might want to provision the sales manager in charge of determining sales territories and sales processes with the Sales Administrator job role in addition to the Sales Manager job role. 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 the topic Creating Rules to Automatically Provision Job Roles to Sales Users.

6. When you create users, the application sends e-mails with the sign-in credentials to the new users unless you disable notifications. You can configure this behavior as described in the topic Managing User-Name and Password Notifications.

Creating a Resource Organization

You must 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 creating manager users in the UI or by importing 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

To create a 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.


4. Click Next.

5. Enter the name of the resource organization in the Name field, for example, Vision Corp. This name will be visible in the resource directory.

   Note the following points:
   - Each resource organization name you enter 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.

6. In the Organization Usages region, click the Add icon and select Sales Organization.

7. Click Finish.
Designating an Organization as the Top of the Sales Hierarchy

After you have created the resource organization for the top person in the sales organization hierarchy, designate that resource organization as the top of the sales hierarchy in the application. If you don’t explicitly designate 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.

Designating the Top of the Sales Hierarchy

To designate a resource organization as the top of the sales hierarchy:

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Resource Organization Hierarchies
3. In the search results, click the Internal Resource Organization Hierarchy link. This value is supplied by Oracle. The View Organization Hierarchy: Internal Resource Organization Hierarchy page appears.
4. From the Action menu, select Edit This Hierarchy Version. The Edit Organization Hierarchy Version page appears.
5. Click Add in the Internal Resource Organization Hierarchy region. The Add Tree Node window appears.
6. Click **Search**.
   The Search Node window appears.
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**.
   The application returns you to the Edit Organization Hierarchy Version page.
10. Click **Save and Close**.
11. When a warning appears, click **Yes**.

**Related Topics**
- Accessing Tasks to Update Existing Setup Data: Procedure

---

### Creating Additional Resource Roles

This topic describes how to create additional resource roles. After you create a resource role, you must create the appropriate provisioning rules to provision the user with the required job and abstract roles. The resource role by itself is only a title.

#### Creating a Resource Role

To 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 to verify that it is necessary to create a new role, then click **Search** without entering search criteria.
   All the available resource roles are listed. Roles that are predefined by Oracle are labeled **System**.
3. Click the **Create** icon to create a new resource role.
   The Create Role page appears.
4. In the **Role Name** field, enter the name of the resource role as it will appear in the application UI, for example, **Inside Sales Representative**.
5. In the **Role Code** field, enter a unique internal name. No spaces are permitted. If you’re importing users from a file then you must include this code in your file rather than the name.
6. Select the **Manager** option if the resource role belongs to a manager, or select the **Member** option if the resource role belongs to an individual contributor such as an inside sales representative.
7. From the **Role Type** list, select **Sales** to classify the role that you’re creating.
8. Click **Save and Close**.

**Related Topics**
- Accessing Tasks to Update Existing Setup Data: Procedure
Creating 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 additional rules you require. You have to create role provisioning rules for any additional resource roles you create, such as an Inside Sales Representative resource role. The provisioning rules use the resource role that you assign to each sales user as the trigger condition for provisioning job roles. Create a separate rule to provision each resource role.

For 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 permits users to access the Resource Directory. Do not add the Resource abstract role for partner roles, including Partner Sales Representative, Partner Sales Manager, and Partner Administrator.

Note: Role provisioning rules are also known as role mappings.

Creating a Provisioning Rule

Perform the steps in the following procedure to review the predefined 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, if you want to review the predefined provisioning rules, do the following:
   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, such as Inside Sales Representative.
   b. Click Search.
      If a role provisioning rule exists for the resource role (either a predefined rule or a rule you created), it is displayed in the Search Results area.
   c. To view or edit a provisioning rule, select the rule from the Search Results area.
      The Edit Role Mapping page is displayed listing details for the rule.

3. To create a new provisioning rule, on the Manage Role Mappings page, click Create.
   The Create Role Mapping page appears.

4. In the Mapping Name field, enter a name that will help you identify the mapping, for example, Inside Sales Representative.

5. In the Conditions region, select the resource role you want to provision from the Resource Role list. For example, if you have created an Inside Sales Representative resource role, select Inside Sales Representative.

6. Select Active from the HR Assignment Status list.
   This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources.
7. In the Associated Roles region, click Add to add the job roles you want to provision. For the Inside Sales Representative, for example, add the Sales Representative job role.

8. For internal sales users, including the Inside Sales Representative, add the Resource abstract role.

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

10. Click Save and Close.

Related Topics

- Accessing Tasks to Update Existing Setup Data: Procedure

Automatic and Manual Role Provisioning

Roles provide user access to data and functions. Roles are assigned to users by defining a relationship, called a role mapping or provisioning rule, between the role and some conditions. Users who satisfy the conditions specified in the mapping are eligible to acquire the role specified in the mapping. This topic describes role mapping options for automatic and manual role provisioning. Predefined provisioning rules are provided with the application but if you need to create new role mappings, you can do so using the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area.

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

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

For example, to create a role mapping rule that automatically provisions the Resource abstract role and the Sales Representative job role to users assigned a resource role, Inside Sales Representative, that you previously created, do the following:

1. Specify the conditions shown in the following table.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Role</td>
<td>Inside Sales Rep.</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

2. Specify the Resource abstract role and the Sales Representative job role for the mapping, and select the Autoprovision option for each.

This mapping rule is applied when the user is first created or when the user’s status or resource role is modified by clicking the Autoprovision Roles option on the Create User or Edit User page.

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 role-mapping.
- You select the Requestable option for the role in the role mapping.
Users can also request a role when managing their own accounts if:

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

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

1. Specify the following conditions for the role mapping.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Role</td>
<td>Sales Operations Manager</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

2. Specify the following roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Autoprovision</td>
</tr>
<tr>
<td>Sales Administrator</td>
<td>Autoprovision</td>
</tr>
<tr>
<td>Customer Data Steward</td>
<td>Requestable</td>
</tr>
<tr>
<td>Sales Representative</td>
<td>Self-requestable</td>
</tr>
</tbody>
</table>

In this example, any user assigned the Sales Operations Manager resource role:

- Is automatically provisioned with the Resource and Sales Administrator roles when the Autoprovision Roles option is clicked 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-Mapping Names**

Role mapping names must be unique in the enterprise. Devise a naming scheme that shows the scope of each role mapping. For example, a role mapping named CEO Autoprovisioned Roles could include all roles provisioned automatically to resources assigned the CEO resource role.

**Enabling Validation of Work Email Values**

You can enable validation of the email that you enter for users on the Create User page. When validation is enabled, a warning message appears if you enter a duplicate value. The message provides the name, the user name, or both of the
email owner. Having this warning enables you to enter a unique email before saving. Email validation on the Create User page is disabled by default. This topic explains how to enable validation.

### Enabling Email Validation

To enable email validation, you create, enable, and set a profile option.

To create and enable the profile option, follow these steps:

1. In the Setup and Maintenance work area, go to the **Manage Profile Options** task.
   
   You can search for the Manage Profile Options task by clicking the **Tasks** panel tab, then selecting **Search**.

2. On the Manage Profile Options page, click the **New** icon in the Search Results section.

3. On the Create Profile Option page, complete the required values as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Option Code</td>
<td>PER_MANAGE_USERS_EMAIL_VALIDATION</td>
</tr>
<tr>
<td>Profile Display Name</td>
<td>Enable Validation of User Work Email</td>
</tr>
<tr>
<td>Application</td>
<td>Sales</td>
</tr>
<tr>
<td>Module</td>
<td>Users</td>
</tr>
<tr>
<td>Start Date</td>
<td>Select the required start date.</td>
</tr>
</tbody>
</table>

4. Click **Save and Close**.

5. In the Profile Option Levels section of the Manage Profile Options page, select the **Enabled** and **Updatable** options at the Site level.

6. Click **Save and Close**.

To set the profile option, follow these steps:

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, click the **New** icon.

4. Enter **Site** in the **Profile Level** field and **Y** in the **Profile Value** field.

5. Click **Save and Close**.

---

** Provisioning Roles for Testing **

---

** ORACLE **
What's Required for Testing Configurations in the Sandbox

If you are creating configurations for a specific job role or if you are creating your own objects, then you must be provisioned with additional job roles to view and test those configurations in the sandbox. You can enable the testing of both types of configurations using the steps described in this section.

What's Required for Role-Specific Configurations

If you are 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 are 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 salespersons, 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 are 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 cannot view or test the objects they create.

Setup Overview

1. While signed in as a user with security privileges, such as the setup user or the initial user you received when you signed up with Oracle, you edit all of the role-provisioning rules 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 are creating your own 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.

   For details, see the Enabling Sales Administrators to Test Configurations in the Sandbox topic.

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 Assigning Yourself an Additional Job Role topic.

Related Topics

• Entering Setup Data Using Assigned Tasks: Procedure
Enabling Sales Administrators to Test Configurations in the Sandbox

Modify the provisioning rules to make it possible for sales administrators to assign themselves the job roles they need for testing configurations in the sandbox. For viewing and testing objects they create, sales 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.

Modifying the Provisioning Rules 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:
   a. Offering: Sales
   b. Functional Area: Users and Security
   c. Task: Manage HCM Role Provisioning Rules

   The Manage Role Mappings page appears.
3. Search for the role mappings that provision the 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 do not want the job roles assigned to the sales administrators automatically.
   c. If you are 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
- Entering Setup Data Using Assigned Tasks: Procedure

Assigning Yourself Additional Job Roles Required for Testing

Sales administrators who are also sales resources can use this procedure to assign themselves the role they must test role-specific modifications in the sandbox. For example, an administrator testing UI modifications for sales managers, requests the Sales Manager job role or the equivalent customer-defined role. If you are creating your own objects, you can use this procedure to assign yourself the Custom Objects Administration role, if this role is not already assigned to you. The Custom Objects Administration role is required for testing your objects in the sandbox.
Assigning Yourself an Additional Job Role

2. Select View Resource Details from the Actions menu in your record.

The Resource page appears.

3. Select the Roles tab.
4. Click Add Role.

The Add Role window appears.

5. 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. It displays in the Current Roles region the next time you navigate to this page.

FAQs for Preparing for Application 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 for which he or she qualifies but doesn’t have
- The user loses any role for which he or she no longer qualifies

It’s recommended that you autoprovision roles to individual users on the Edit User page when new or changed role mappings exist. 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 provision to a user?

You can provision a role if a role mapping exists for the role, the Requestable option is selected for the role in the role mapping, and at least one of your assignments satisfies the role-mapping conditions. Otherwise, you can’t provision the role to other users.

Can I implement single sign-on in the cloud?

Yes. Single sign-on enables users to sign in once but access multiple applications, within and across product families.
Submit a service request for implementation of single sign-on. For more information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at https://support.oracle.com.
Creating Sales Users

User Setup Options

This topic describes the enterprise options that are available for controlling default functionality when users are created in the application. You might have made decisions about user setup options when you configured your application security environment and set up the Security Console. If you did not, then it’s recommended that you configure these options before you start to create users.

To review user setup options, navigate to the Administration tab of the Security Console. For detailed information about configuring the options, see the chapter Setting Up Applications Security.

User Name and Password Notifications

By default, users automatically receive an e-mail notification containing their sign-in details when their user account is created. You can edit the text of the e-mail notification the user receives or suppress e-mail 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.

Default User Name Format

You can select the default format used to generate user names for application users in cases where a user name is not specified. Unless you specify otherwise, the default format is e-mail address.

Related Topics
- Setting the Default User-Name Format: Procedure
- Setting Password Policy: Explained

Creating Application Users

This topic describes how to create users in the application UI using the Manage Users work area. Use this method of creating users to create individual application users.

You can also create users by importing users from a file using the file import functionality. Importing users from a file is useful when you have a large number of users to create. For additional information, see the chapter about importing employee resources in the file-based data import guide on the Oracle Help Center (https://docs.oracle.com/).

Before creating application users, make sure you have:
- Set up any additional resource roles or role provisioning rules that are required.
- Created 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 with his or her own resource organization. Individual contributors automatically inherit their manager’s resource organization. The application determines who is 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.

Steps to Create an Application User

Use the following procedure to create users in the UI. Note that the procedure is slightly different for managers and individual contributors:

- You must assign each manager with his or her own resource organization. You can create the resource organization while creating the manager.
- Individual contributors automatically inherit their managers’ resource organization.

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

To create a 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.
   The Create User page opens.
3. In the Personal Details region, enter the user’s name and a unique e-mail address. The application sends user notifications to this e-mail address by default unless you disable notifications in the Security Console.

   **Note:** After you create the user, if you want to change the e-mail address you can do so on the Users tab of the Security Console or using file import. You can’t change e-mail 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 are 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 are allocating monthly quotas for fiscal year July 01, 2015 to June 30, 2016, then you must enter a hire date of 7-1-2015 or earlier. You cannot 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 are 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, e-mail address is the default user name format.
   - Alternatively, if you want to link the new person record you are 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 to select whether or not you want a notification containing the new user’s login details to be sent to the user when the user account is created.
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 e-mail later by running the Send User Name and Password E-Mail Notifications process. The process sends out user names and reset-password links to any users for whom you haven’t so far requested an e-mail. 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.

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

You don’t have to complete the remaining fields in the Employment Information region.

8. In the Resource Information region, enter the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Role</td>
<td>Select the role the user plays in the resource organization.</td>
</tr>
<tr>
<td>Reporting Manager</td>
<td>Select the user’s manager. If you are creating the top user in your hierarchy, such as the CEO, you can leave this field blank.</td>
</tr>
<tr>
<td>Organization</td>
<td>If the user you are 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 <strong>Create</strong> link from the end of the <strong>Organization</strong> list. The <strong>Create Organization</strong> dialog box is displayed allowing you to enter a new organization name. If the user you are creating is not a manager, then the resource organization is automatically copied from the manager.</td>
</tr>
</tbody>
</table>

9. 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.
You can also provision a role manually to the user if required by clicking **Add Role**. The **Add Role** dialog box opens. 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.

12. Click **Save and Close**.
   The application creates the user. If you selected the **Send user name and password** option, the application also sends the e-mail with the user’s login details.

13. Click **Done**.

**Related Topics**
- Creating a Resource Organization: Worked Example
- About Sales Users: Explained

## Creating Sales 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.

### Creating Sales Restricted Users

To create a sales restricted user:

1. Create the user who is to have restricted access to the application.
   For information about this task, see the topic Creating Sales Application Users.

2. When creating the user, specify the values shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>Resource Role</td>
<td>Sales Restricted User</td>
</tr>
</tbody>
</table>

3. In the Roles region, click **Autoprovition 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.
10 Managing Sales Users

Managing Users: Overview

This chapter describes user management tasks you have to perform on an on-going basis. These tasks include:

- Resetting passwords for users
- 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

Note: 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 (Settings and Actions > Set Preferences).

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

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

For additional information, see the chapter about importing employee resources in the guide Understanding File-Based Data Import and Export at http://docs.oracle.com.

Resetting Passwords for Users

Setup users, who are provisioned with the IT Security Manager job role, can use the Users tab in the Security Console work area to reset passwords for all application users.

Note: Users who cannot access the Security Console can only reset their own passwords by clicking the Set Preferences link in the Settings and Actions menu (available by clicking your user name) or by using Forgot Password on the sign-in page.

To reset a user’s password in the Security Console:

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Applications Security Preferences
2. In the Security Console, you can ignore and close any warnings regarding the scheduling of the Import Users and Roles Application Security Data job.
3. Click the Users tab.
4. On the User Accounts page, search for the user using one of the following:
   o First or last name, but not both
   o User name

5. From the Action menu for the user, select Reset Password. The Reset Password window is displayed.

6. 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.

7. To reset the password yourself, do the following:
   a. Select the Manually change the password option.
   b. Enter the new password twice.

   Note: The option to reset a password to an automatically generated value is always available. To enable the manual-reset option, you must select the option Administrator can manually reset password on the Password Policy subtab of the User Categories page on the Security Console.

8. Click Reset Password.

Related Topics
• Accessing Tasks to Update Existing Setup Data: Procedure

Changing a User's E-Mail Address

Use the Users tab in the Security Console work area to change user email addresses. If you’re updating the email addresses of sales users, then you can also use the same import process you use to create them.

1. Navigate to the Security Console.
2. Click the Users tab.
3. Search for the user using one of the following:
   o First or last name, but not both
   o 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.

Changing 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 this value can be overridden for the enterprise. 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 as described in this topic.

Existing User Names
To change an existing user name, sign in to the application as a setup user, then perform the following 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.

**Tip:** When you change an existing user name on the Edit User page, the user's password and roles remain the same. However, the user doesn't receive an automatic notification of the change. Therefore, it's recommended that you send details of the updated user name directly to the user.

Changing User Resource Roles When Job Assignments Change
If an employee takes on a different role within the company, for example, if the employee is promoted, then you must update the resource role assigned to the employee. Changing the resource role assigned to an employee involves the following steps:

- Assigning the user a new resource role that corresponds to the new 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 file import 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 are updating resource role information for an individual user, then using the UI can be more efficient.

The following procedure describes how to update role information in the UI for a user who is 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 is 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 as follows:

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 does not change. That is, any users who reported to the Sales Manager continue to report to the same individual when he or she 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.

Terminating User Accounts

This topic describes how to terminate a user account when an employee leaves your company. You cannot delete a sales user account using the Security Console. However, when an employee leaves your company, you can suspend the user account by completing the following steps in the Manage Users and Manage Resources work areas:

1. Perform either one of the following tasks:
   o Inactivate the user’s account.
   o Remove the user’s roles.

2. Set an end date for the resource.

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

Note: When you deactivate a user account, the user record is not 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 is recommended that you inactivate the user account. Inactivating the user’s account prevents the user from being able to log in to the application.

To inactivate a user account, perform the following steps:

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

To selectively remove roles from a user, perform the following steps:

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.

To set the end date for a user, perform the following steps:

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

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

Related Topics
- Accessing Tasks to Update Existing Setup Data: Procedure

FAQs for Terminating Users

How are the records of a terminated employee reassigned?

After you terminate an employee in the application, the assignment process automatically excludes the terminated user when
it runs again. However, you have to manually handle other reassignments, for example, replacing the terminated user with
another user on the territory team or sales account 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
- Transferring Records Between Users: Procedure
- Transferring Records Between Users: Explained

Can I reactivate a terminated employee record?

Yes. After you have specified an end date for a resource, you can’t reverse it in the sales application. However, 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.

Impersonation and Proxy Users
Privileges Required by Proxy Users

The impersonation functionality in the sales application allows you to designate another user as a proxy to sign in to the application and perform tasks on your behalf. For example, a channel manager might want to log into the Partner Portal as a partner user to resolve a query relating to the UI pages or data.

Channel managers do not require a partner user's permission to impersonate the partner user. To implement impersonation in all other cases, however:

- The user must explicitly designate another user as his or her proxy.
- The designated user must have the privileges required to act as a proxy.

Impersonate User Privilege

You can select a user to act as your proxy only if the user has the privilege required to be a proxy, that is, the Impersonate User privilege. The following job roles are assigned the Impersonate User privilege by default; therefore, users assigned these job roles can act as proxies for other users:

- Channel Account Manager
- Channel Operations Manager

You can enable other groups of users to act as proxies by creating a copy of the job role assigned to the users and adding the Impersonate User privilege to the copied custom role.

Note: When deciding whether or not to assign the Impersonate User privilege to an additional job role, be aware that a proxy user can access all the same data and tasks as the user they impersonate.

Related Topics

- Impersonating a Partner User: Explained
- Copying Job or Abstract Roles: Procedure

Configuring Impersonation Auditing

The impersonation functionality allows users to temporarily designate another user as a proxy to sign in to the application on their behalf. A proxy user has the same privileges as the impersonated user and has access to all of the impersonated user’s personal data. By default, therefore, auditing of proxy user sessions is enabled, even when auditing is disabled for the application. An audit record tracks the user name of the proxy and any transactions performed.

Auditing of proxy sessions is recommended but, if appropriate for your environment, you can disable impersonation auditing by changing the default value of the site-level profile option Audit Impersonation Transaction Enabled.

Note: A number of database tables aren’t enabled for impersonation transaction auditing. If impersonation auditing is enabled, proxy users can’t save transactions that result in changes to the data in those tables. If the administrator disables impersonation auditing using the Audit Impersonation Transaction Enabled profile option, proxy users can change the data in any tables, whether or not the tables are enabled for impersonation auditing.

For additional information about auditing in the sales application, including information about the objects that can be enabled for auditing, see the Implementing Sales guide on Oracle Help Center at http://docs.oracle.com/.
Configuring Impersonation Auditing
The following procedure describes how to enable or disable impersonation auditing functionality by changing the value of the Audit Impersonation Transaction Enabled profile option.

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, in the Search: Profile Option section, enter **Audit Impersonation Transaction Enabled** in the **Profile Display Name** field.

3. Click **Search**.

4. In the Search Results list, select **FND_AUDIT_IMPERSONATION_TRANSACTIONS**.

5. In the FND_AUDIT_IMPERSONATION_TRANSACTIONS: Profile Values section, select the Site Profile level and set the value of the **Profile Value** field to either **Yes** or **No**.

6. Click **Save and Close**.

Related Topics

- [Accessing Tasks to Update Existing Setup Data: Procedure](#)
11 Reporting on Application Users and Roles

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console. This report is based on data in the Applications Security tables, which you populate by running the Import User and Role Application Security Data process.

To run the User and Role Access Audit Report:

1. In the Scheduled Processes work area, click Schedule New Process.
2. Search for and select the User and Role Access Audit Report process.
3. In the Process Details dialog box, set parameters and click Submit.
4. Click OK to close the confirmation message.

User and Role Access Audit Report Parameters

Population Type

Set this parameter to one of these values to run the report for one user, one role, multiple users, or all roles.

- All roles
- Multiple users
- Role name
- User name

User Name

Search for and select the user name of a single user.

This field is enabled only when Population Type is User name.

Role Name

Search for and select the name of a single aggregate privilege or data, job, abstract, or duty role.

This field is enabled only when Population Type is Role name.

From User Name Starting With

Enter one or more characters from the start of the first user name in a range of user names.

This field is enabled only when Population Type is Multiple users. It enables you to report on a subset of all users.

To User Name Starting With

Enter one or more characters from the start of the last user name in a range of user names.

This field is enabled only when Population Type is Multiple users. It enables you to report on a subset of all users.
**User Role Name Starts With**

Enter one or more characters from the start of a role name.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of all users and roles.

**Data Security Policies**

Select **Data Security Policies** to view the data security report for any population. If you leave the option deselected, then only the function security report is generated.

> Note: If you don’t need the data security report, then leave the option deselected to reduce the report processing time.

**Debug**

Select **Debug** to include the role GUID in the report. The role GUID is used to troubleshoot. Select this option only when requested to do so by Oracle Support.

**Viewing the Report Results**

The report produces either one or two .zip files, depending on the parameters you select. When you select **Data Security Policies**, two .zip files are generated, one for data security policies and one for functional security policies in a hierarchical format.

The file names are in the following format: `[FILE_PREFIX][PROCESS_ID][DATE][TIME][FILE_SUFFIX]`. The file prefix depends on the specified **Population Type** value.

This table shows the file prefix values for each report type.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>USER_NAME</td>
</tr>
<tr>
<td>Role name</td>
<td>ROLE_NAME</td>
</tr>
<tr>
<td>Multiple users</td>
<td>MULTIPLE_USERS</td>
</tr>
<tr>
<td>All roles</td>
<td>ALL_ROLES</td>
</tr>
</tbody>
</table>

This table shows the file suffix, file format, and file contents for each report type.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Suffix</th>
<th>File Format</th>
<th>File Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>DataSec</td>
<td>CSV</td>
<td>Data security policies. The .zip file contains one file for all users or roles. The data security</td>
</tr>
</tbody>
</table>
### User Role Membership Report

The User Role Membership Report lists role memberships for specified users.

To run the report process:

1. Open the Scheduled Processes work area.
2. Search for and select the **User Role Membership Report** process.

#### User Role Membership Report Parameters

You can specify any combination of the following parameters to identify the users whose role memberships are to appear in the report.

* **Note:** The report may take a while to complete if you run it for all users, depending on the number of users and their roles.

#### User Name Begins With
Enter one or more characters of the user name.

**First Name Begins With**
Enter one or more characters from the user’s first name.

**Last Name Begins With**
Enter one or more characters from the user’s last name.

**Department**
Enter the department from the user’s primary assignment.

**Location**
Enter the location from the user’s primary assignment.

### Viewing the Report

The process produces a UserRoleMemberships_processID_CSV.zip file and a Diagnostics_processID.zip file. The UserRoleMemberships_processID_CSV.zip file contains the report output in CSV format. The report shows the parameters that you specified, followed by the user details for each user in the specified population. The user details include the user name, first and last names, user status, department, location, and role memberships.

### User Password Changes Audit Report

This report identifies users whose passwords were changed in a specified period. You must have the ASE_USER_PASSWORD_CHANGES_AUDIT_REPORT_PRIV function security privilege to run this report. The predefined IT Security Manager job role has this privilege by default.

To run the User Password Changes Audit Report:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the **User Password Changes Audit Report** process.
4. In the Process Details dialog box, set parameters and click **Submit**.
5. Click **OK** to close the confirmation message.

### User Password Changes Audit Report Parameters

**Search Type**
Specify whether the report is for all users, a single, named user, or a subset of users identified by a name pattern that you specify.

**User Name**
Search for and select the user on whom you want to report. This field is enabled only when Search Type is set to Single user.

**User Name Pattern**

Enter one or more characters that appear in the user names on which you want to report. For example, you could report on all users whose user names begin with the characters SAL by entering SAL%. This field is enabled only when Search Type is set to User name pattern.

**Start Date**

Select the start date of the period during which password changes occurred. Changes made before this date don't appear in the report.

**To Date**

Select the end date of the period during which password changes occurred. Changes made after this date don't appear in the report.

**Sort By**

Specify how the report output is sorted. The report can be organized by either user name or the date when the password was changed.

**Viewing the Report Results**

The report produces these files:

- UserPasswordUpdateReport.csv
- UserPasswordUpdateReport.xml
- Diagnostics_[process ID].log

For each user whose password changed in the specified period, the report includes:

- The user name.
- The first and last names of the user.
- The user name of the person who changed the password.
- How the password was changed:
  - ADMIN means that the change was made for the user by a line manager or the IT Security manager, for example.
  - SELF_SERVICE means that the user made the change by setting preferences or requesting a password reset, for example.
  - FORGOT_PASSWORD means that the user clicked the Forgot Password link when signing in.
- The date and time of the change.
Inactive Users Report

Run the **Inactive Users Report** process to identify users who haven’t signed in for a specified period.

To run the report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **Import User Login History** process.

   **Note:** Whenever you run the **Inactive Users Report** process, you must first run the **Import User Login History** process. This process imports information that the **Inactive Users Report** process uses to identify inactive users. You’re recommended to schedule **Import User Login History** to run daily.

3. When the **Import User Login History** process completes, search for and select the **Inactive Users Report** process.
4. In the Process Details dialog box, set parameters to identify one or more users.
5. Click **Submit**.

**Inactive Users Report Parameters**

All parameters except **Days Since Last Activity** are optional.

**User Name Begins With**

Enter one or more characters.

**First Name Begins With**

Enter one or more characters.

**Last Name Begins With**

Enter one or more characters.

**Department**

Enter the department from the user’s primary assignment.

**Location**

Enter the location from the user’s primary assignment.

**Days Since Last Activity**

Enter the number of days since the user last signed in. Use this parameter to specify the meaning of the term inactive user in your enterprise. Use other parameters to filter the results.

This value is required and is 30 by default. This value identifies users who haven’t signed in during the last 30 or more days.

**Last Activity Start Date**
Specify the start date of a period in which the last activity must fall.

**Last Activity End Date**

Specify the end date of a period in which the last activity must fall.

### Viewing the Report

The process produces an `Inactive_Users_List_processID.xml` file and a `Diagnostics_processID.zip` file.

The report includes the following details for each user who satisfies the report parameters:

- Number of days since the user was last active
- Date of last activity
- User name
- First and last names
- Assignment department
- Assignment location
- City and country
- Report time stamp

> **Note:** The information in the report relating to the user's latest activity isn't based solely on actions performed by the user in the UI. Actions performed on behalf of the user, which create user sessions, also affect these values. For example, running processes, making web service requests, and running batch processes are interpreted as user activity.

### Related Topics

- Importing User Login History: Explained

### User History Report

This topic describes the User History report, which extracts and formats the history of a specified user account. Oracle Support might ask you to run this report to help diagnose user-related errors. To run the report, you must inherit the `ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI` (Manage Users) duty role. Several predefined job roles, including IT Security Manager, inherit this duty role.

Follow these steps to run the report.

1. Select **Navigator > My Team > Users and Roles**.
2. On the Search Person page, search for the person of interest.
3. In the search results, click the person name to open the Edit User page.
4. On the Edit User page, click **Print User History**. In the **User History** dialog box, you can review the report.
   
   You can either print the report or download a PDF file by clicking relevant icons in the **User History** dialog box.
5. Click **Cancel** to close the **User History** dialog box.

**Tip:** You don’t have to view the report. You can select **Print User History > Download** to download the PDF file. The file name is in the format `<person ID>_UserHistory.pdf.

This report is identical to the HCM Person User Information report, which authorized users can run in the HCM Reports and Analytics work area. Information is provided in this report for sales resources who are also defined as users in HCM.

**Report Contents**

For the selected user, the report includes:

- Person information
- User history
- Provisioned roles and details of any associated role mappings
- Role delegation details
- LDAP request details
- Work relationship and assignment information
12 Using the Security Console to Review and Analyze Roles

Reviewing Roles on the Security Console: Overview

This chapter describes how to use the Security Console to review and analyze role information. You perform these tasks from the Roles and Analytics tabs of the Security Console.

You can perform the following tasks from the Roles tab:

- Visualize role hierarchies and role assignments to users.
- Review Navigator menus available to roles or users, identifying roles that grant access to Navigator items and privileges required for that access.
- Compare roles.
- Copy roles, create roles, and edit custom job, abstract, and duty roles.

For information on copying roles and creating roles, see the chapter Creating Job, Abstract, and Duty Roles.

From the Analytics tab, you can:

- Review statistics concerning role categories, the roles belonging to each category, and the components of each role.
- View the data security policies, roles, and users associated with each database resource.

Graphical and Tabular Role Visualizations

On the Roles tab, you can review role hierarchies. You can choose whether to display role hierarchies using either a tabular or a graphical view. The view you see by default depends on the setting of the Enable default table view option on the Administration tab. This topic describes how to use each of these views.

Role hierarchies stretch from users at the top of the hierarchy to privileges at the bottom. In both graphical and tabular views, you can set the direction of the displayed hierarchy.

- To show from the selected user, role, or privilege up the hierarchy, set Expand Toward to Users.
- To show from the selected user, role, or privilege down the hierarchy, set Expand Toward to Roles.

The Tabular View

If the tabular view doesn't appear when you select a security artifact on the Roles tab, then you can click the View as Table icon. In the tabular view, you can:

- Review the complete role hierarchy for a selected user or role. The table shows roles inherited both directly and indirectly.
- Search for a security artifact by entering a search term in the column search field and pressing Enter.
Set the contents of the table as follows:

- If Expand Toward is set to Privileges, then you can set Show to either Privileges or Roles.
- If Expand Toward is set to Users, then you can set Show to either Roles or Users.

The resulting contents of the table depend on the start point. For example, if you select a privilege, Expand Toward is set to Privileges, and Show is set to Roles, then the table is empty.

Export the displayed details to a Microsoft Excel spreadsheet.

### The Graphical View

If the graphical view doesn’t appear when you select a security artifact on the Roles tab, then you can click the Show Graph icon. In the graphical view, users, privileges, and the various types of roles are represented by nodes and differentiated by both color and labels. These values are defined in the Legend. You can:

- Review roles inherited directly by the selected role or user. To see roles and privileges inherited indirectly, select a directly inherited role, right-click, and select either Expand or Expand All. Select Collapse or Collapse All to reverse the action. Alternatively, double-click a node to expand or collapse it.
- Use the Set as Focus action to make any selected node the center of the visualization.
- Use the Overview icon to manipulate the visualization. For example, clicking a node in the Overview moves the node to the center of the visualization. You can also use drag and drop.
- Hover on a legend entry to highlight the corresponding nodes in the visualization. Click a legend entry to add or remove corresponding nodes in the visualization.

In the Control Panel, you can:

- Switch the layout between radial and layered representations.
- Click the Search icon and enter a search term to find a security artifact among currently displayed nodes.
- Zoom in and out using either the Zoom in and Zoom out icons or the mouse wheel.
- Magnify areas of the visualization by clicking the Magnify icon and dragging it to the area of interest. Click the icon again to switch it off.
- Click the Zoom to Fit icon to center the image and fill the display area.

### Reviewing Role Hierarchies

On the Security Console you can review the role hierarchy of a job role, an abstract role, or a duty role. You must have the IT Security Manager job role to perform this task.

To review a role’s hierarchy:

1. On the Roles tab of the Security Console, ensure that Expand Toward is set to Privileges.
2. Search for and select the role.

   Depending on the enterprise setting, either a table or a graphical representation of the role is displayed.

3. If the table doesn’t appear by default, click the View as Table icon.

   The table lists every role inherited either directly or indirectly by the selected role. To view the privileges inherited by the role, set the Show field to Privileges.
Tip: Enter text in a column search field and press Enter to show only those roles or privileges that contain the specified text.

4. Click Export to Excel to export the current table data to Microsoft Excel.

Simulating Navigator Menus in the Security Console

You can simulate Navigator menus available to roles or users. From a simulation, you can review the access inherent in a role or granted to a user. You can also determine how to alter that access to create roles.

Opening a Simulation
To open a simulated menu:

1. Select the Roles tab in the Security Console.
2. Create a visualization graph, or populate the Search Results column with a selection of roles or users.
3. In the visualization graph, right-click a role or user. Or, in the Search Results column, select a user or role and click its menu icon.
4. Select Simulate Navigator.

Working with the Simulation
In a Simulate Navigator page:

- Select Show All to view all the menu and task entries that may be included in a Navigator menu.
- Select Show Access Granted to view the menu and task entries actually assigned to the selected role or user.

In either view:

- A padlock icon indicates that a menu or task entry can be, but is not currently, authorized for a role or user.
- An exclamation icon indicates an item that may be hidden from a user or role with the privilege for it, because it has been modified.

To plan how this authorization may be altered:

1. Click any menu item on the Simulate Navigator page.
2. Select either of the two options:
   - View Roles That Grant Access: Lists roles that grant access to the menu item.
   - View Privileges Required for Menu: Lists privileges required for access to the menu item.

Reviewing Role Assignments
You can use the Security Console to:

- View the roles assigned to a user.
- Identify users who have a specific role.

You must have the IT Security Manager job role to perform these tasks.

### Viewing the Roles Assigned to a User

Follow these steps:

1. Open the Security Console.
2. On the Roles tab, search for and select the user.

   Depending on the enterprise setting, either a table or a graphical representation of the user’s role hierarchy appears. Switch to the graphical representation if necessary to see the user and any roles that the user inherits directly. User and role names appear on hover. To expand an inherited role:
   
   a. Select the role and right-click.
   b. Select Expand. Repeat these steps as required to move down the hierarchy.

   **Tip:** Switch to the table to see the complete role hierarchy at once. You can export the details to Microsoft Excel from this view.

### Identifying Users Who Have a Specific Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select the role.
2. Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn’t appear by default.
3. Set **Expand Toward** to **Users**.

   **Tip:** Set the **Expand Toward** option to control the direction of the graph. You can move either up the hierarchy from the selected role (toward users) or down the hierarchy from the selected role (toward privileges).

   In the refreshed graph, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. Expand a role to view its hierarchy.

4. In the Legend, click the **Tabular View** icon for the **User** icon. The table lists all users who have the role. You can export this information to Microsoft Excel.

### Comparing Roles

You can compare any two roles to see the structural differences between them. As you compare roles, you can also add function and data security policies existing in the first role to the second role, providing that the second role is not a predefined role.

For example, assume you have copied a role and edited the copy. You then upgrade to a new release. You can compare your edited role from the earlier release with the role as shipped in the later release. You may then decide whether to incorporate upgrade changes into your edited role. If the changes consist of new function or data security policies, you can upgrade your edited role by adding the new policies to it.
Selecting Roles for Comparison

1. Select the Roles tab in the Security Console.
2. Do any of the following:
   - Click the Compare Roles button.
   - Create a visualization graph, right-click one of its roles, and select the Compare Roles option.
   - Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select Compare Roles.
3. Select roles for comparison:
   - If you began by clicking the Compare Roles button, select roles in both First Role and Second Role fields.
   - If you began by selecting a role in a visualization graph or the Search Results column, the First Role field displays the name of the role you selected. Select another role in the Second Role field.

For either field, click the search icon, enter text, and select from a list of roles whose names contain that text.

Comparing Roles

1. Select two roles for comparison.
2. Use the Filter Criteria field to filter for any combination of these artifacts in the two roles:
   - Function security policies
   - Data security policies
   - Inherited roles
3. Use the Show field to determine whether the comparison returns:
   - All artifacts existing in each role
   - Those that exist only in one role, or only in the other role
   - Those that exist only in both roles
4. Click the Compare button.

You can export the results of a comparison to a spreadsheet. Select the Export to Excel option.

After you create the initial comparison, you can change the filter and show options. When you do, a new comparison is generated automatically.

Adding Policies to a Role

1. Select two roles for comparison.
   - As the First Role, select a role in which policies already exist.
   - As the Second Role, select the role to which you are adding the policies. This must be a custom role. You cannot modify a predefined role.
2. Ensure that your selection in the Filter Criteria field excludes the Inherited roles option. You may select Data security policies, Function security policies, or both.
3. As a Show value, select Only in first role.
4. Click the Compare button.
5. Among the artifacts returned by the comparison, select those you want to copy.
6. An Add to Second Role option becomes active. Select it.

Role Analytics

You can review statistics about the roles that exist in your Oracle Cloud instance. Select the Analytics tab, and then the Roles tab on the Analytics page. Then view these analyses:

- Role Categories. Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example "Financials - Duty Roles."

  For each category, a Roles Category grid displays the number of:
  - Roles
  - Role memberships (roles belonging to other roles within the category)
  - Security policies created for those roles

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.

- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:
  - Role memberships
  - Security policies
  - Users assigned the role

- Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

Click Export to export data from this page to a spreadsheet.

Security Console Analytics for Database Resources

You can review information about data security policies that grant access to a database resource, or about roles and users granted access to that resource.

To begin, select the Analytics tab, and then the Database Resources tab on the Analytics page. Select the resource you want to review in the Database Resource field. Then click Go. Results are presented in three tables.

Data Security Policies

The Data Security Policies table documents policies that grant access to the selected database resource.

Each row documents a policy, specifying by default:

- The data privileges it grants.
• The condition that defines how data is selected from the database resource.
• The policy name and description.
• A role that includes the policy.

For any given policy, this table may include multiple rows, one for each role in which the policy is used.

Authorized Roles
The Authorized Roles table documents roles with direct or indirect access to the selected database resource. Any given role may:

• Include one or more data security policies that grant access to the database resource. The Authorized Roles table includes one row for each policy belonging to the role.
• Inherit access to the database resource from one or more roles in its hierarchy. The Authorized Roles table includes one row for each inheritance.

By default, each row specifies:

• The name of the role it documents.
• The name of a subordinate role from which access is inherited, if any. (If the row documents access provided by a data security policy assigned directly to the subject role, this cell is blank.)
• The data privileges granted to the role.
• The condition that defines how data is selected from the database resource.

**Note:** A role’s data security policies and hierarchy may grant access to any number of database resources. However, the Authorized Roles table displays records only of access to the database resource you selected.

Authorized Users
The Authorized Users table documents users who are assigned roles with access to the selected database resource.

By default, each row specifies a user name, a role the user is assigned, the data privileges granted to the user, and the condition that defines how data is selected from the database resource. For any given user, this table may include multiple rows, one for each grant of access by a data security policy belonging to, or inherited by, a role assigned to the user.

Manipulating the Results
In any of these three tables, you can:

• Add or remove columns. Select **View - Columns**.
• Search among the results. Select **View - Query by Example** to add a search field on each column in a table.
• Export results to a spreadsheet. Select the **Export to Excel** option available for each table.
Creating Job, Abstract, and Duty Roles

Security Configuration: Overview

This chapter describes some of the ways in which you can configure the predefined sales security model.

The Oracle implementation of role-based access control is designed to handle a wide range of security requirements in different environments. As a result, most companies can use the standard security settings without modification. If necessary, however, you can configure the default settings to meet specific business requirements. For example, you can create your own roles and role hierarchies. Before making any changes to the security reference implementation, however, do the following:

- Clearly define the change that is required and review the proposed changes with Oracle Support.
- Make sure you understand the interrelationships of the various security components and the effect of the proposed change on user access.
- Document any changes you make.

For additional information about changing the standard security settings, go to the Security Resource Center, which is available at 1609084.1 (Article ID) on My Oracle Support. The Security Resource Center provides templates you can use to track the changes you make to standard settings.

Copying Sales Roles: Points to Consider

Copying predefined roles and editing the copies is the recommended approach to creating roles. This topic describes some of the issues to consider when copying a role on the Security Console.

**Note:** You can copy the predefined roles but can’t edit them. Predefined roles have role codes with the prefix `ORA_`.

Role-Copy Options

When you copy a role on the Security Console, you have the option of copying the top role only (shallow copy), or of copying the top role and its inherited roles (deep copy). The result of selecting each of these copy options is described in this section.

- Copying the Top Role

  If you select the **Copy top role** option, you copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. Subsequent changes to the inherited roles affect not only the source top role, but also your copy. The result of selecting the Copy top role option, therefore, is as follows:

    - You can add roles directly to the copied role without affecting the source role.
    - You can remove any role that’s inherited directly by the copied role without affecting the source role.
    - If you remove any role that’s inherited indirectly by the copied role, then the removal affects both the copied role and any other role that inherits the removed role’s parent role, including the source role.
If you edit any inherited role, then the changes affect any role that inherits the edited role. The changes aren’t limited to the copied role.

To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. You can either select the Copy top role and inherited roles option or copy individual inherited roles separately, edit the copies, and use them to replace the existing versions.

- Copying the Top Role and Inherited Roles

If you select the Copy top role and inherited roles option, you copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the top role is connected to new copies of subordinate roles.

Note: Inherited duty roles are copied if a copy of the role with the same name doesn’t already exist. Otherwise, the copied role inherits links to the existing copies of the duty roles.

When inherited duty roles are copied, you can edit them without affecting other roles. Equally, changes made subsequently to duty roles in the source role hierarchy aren’t reflected in the copied role.

Reviewing the Role Hierarchy

When you copy a predefined job, abstract or duty role, it's recommended that you first review the role hierarchy to identify any inherited roles that you want to either copy, add, or delete in your custom role. You can review the role hierarchy on the Roles tab of the Security Console in either graphical or tabular format. You can also:

- Export the role hierarchy to a spreadsheet from the Roles tab.
- Review the role hierarchy and export it to a spreadsheet from the Analytics tab.
- Run the User and Role Access Audit Report.

Job and abstract roles inherit function security privileges and data security policies from the roles that they inherit. Function security privileges and data security policies may also be granted directly to a job or abstract role. Review these directly granted privileges on the Roles tab of the Security Console, as follows:

- In the graphical view of a role, its inherited roles and function security privileges are visible at the same time.
- In the tabular view, you set the Show value to switch between roles and function security privileges. You can export either view to a spreadsheet.

Once your custom role exists, edit it to add or remove directly granted function security privileges.

Note: Data security policies are visible only when you edit your role; they don’t display in the graphical or tabular role views. However, you can view the data security policies assigned to a role from the Analytics tab of the Security Console.

Report and Analytics Roles

You cannot copy roles that are used to secure sales analytics and reports. Therefore you cannot copy any of the following types of roles:

- Transaction Analysis Duty roles
- Business Intelligence roles
- Any role with a role code prefix of OBIA, for example, OBIA_ANALYSIS_GENERIC_DUTY
You can however, add any of these roles to custom job roles that you create.

### Naming Copied Roles

By default, a copied role has the same name as its source role with the suffix **Custom**. The role codes of copied roles have the suffix **_CUSTOM**. Copied roles lose the prefix **ORA**_ automatically from their role codes. You can define a local naming convention for custom roles, with a prefix, suffix, or both, on the Roles subtab of the Security Console Administration tab.

> **Note:** Copied roles take their naming pattern from the default values specified on the Roles subtab of the Security Console Administration tab. You can override this pattern on the Copy Role: Basic Information page for the role that you’re copying. However, the names of roles inherited by the copied role are unaffected. For example, if you perform a deep copy of the Employee role, then duty roles inherited by that role take their naming pattern from the default values.

If any role in the hierarchy already exists when you copy a role, then no copy of that role is made. For example, if you make a second copy of the Employee role, then copies of the inherited duty roles might already exist. In this case, the copied role inherits links to the existing copies of the roles. To create unique copies of inherited roles, you must enter unique values on the Administration tab of the Security Console before you perform a deep copy. To retain links to the predefined job or abstract role hierarchy, perform a shallow copy of the predefined role.

**Related Topics**

- Setting Role Preferences: Explained

### Copying Job or Abstract Roles

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch, especially if your changes are minor. This topic explains how to copy a role to create a new role. You must have the IT Security Manager job role to perform this task.

> **Note:** You can identify predefined job and abstract roles easily by their role codes, which have the prefix **ORA**_.

### Copying a Role

To copy a job or abstract role:

1. On the Roles tab of the Security Console, search for the role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

   > **Tip:** Click the Show Graph icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.
Tip: 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. You can overwrite these values for the role that you’re copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the Summary and Impact Report train stop.
8. Click Submit and Close, then OK to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is Complete, you can edit the copied role.

Editing Job or Abstract Roles

You can create a role by copying a predefined job role or abstract role and then editing the copy. This topic describes how to edit a role on the Security Console. You must have the IT Security Manager job role to perform this task.

Editing 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.
4. Click Next.

Managing Functional Security Privileges

On the Edit Role: Function Security Policies page, any functional 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 is 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.
   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. As you can’t grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can’t edit these values.
Managing 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 the topic Editing Data Security Policies on the Security Console.

Click Next to continue to the next page.

Adding and Removing Inherited Roles
The Edit Role: Role Hierarchy page shows the copied role and its inherited duty roles. The hierarchy is in tabular format by default but you can switch to graphical mode. 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.

Assigning the Role to Users
On the Edit Role: Users page you can assign the copied role to users.

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.
Reviewing the Role

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

1. Click Back to make corrections.
2. When you have 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.

Creating Job or Abstract Roles

If the predefined job or abstract roles don’t meet enterprise requirements, then you can create new job or abstract roles. In many cases, an efficient method of creating a role is to copy an existing role, then edit the copy to meet your requirements. However, if the predefined roles aren’t similar enough to the roles that you require, then you can create a job role or abstract role from scratch as described in this topic. To perform this task, you must have the IT Security Manager job role.

Entering Basic Information

To create the new role, perform the following steps:

1. On the Roles tab of the Security Console, click Create Role.
2. On the Create Role: Basic Information page, enter the role’s display name in the Role Name field. For example, enter Inside Sales Representative.
3. Enter a unique Role Code value. For example, enter INSIDE_SALES_REP_JOB.
   Abstract roles have the suffix _ABSTRACT, and job roles have the suffix _JOB.
4. In the Role Category field, select the appropriate role category, for example, CRM - Job Roles.
5. Click Next.

Adding Functional Security Policies

When you create a role from scratch, you’re most likely to add one or more duty roles to your role. You’re less likely to grant function security privileges directly to the role. If you aren’t granting function security privileges, then click Next.

To grant function security privileges to the new role:

2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
   You can either add an individual privilege or copy all the privileges that belong to an existing role.
3. If you select a role, then click Add Selected Privileges to add all the function security privileges assigned to the selected 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.

All the privileges you added are listed on the Create Role: Functional Security Policies page. You can:

- Click on a privilege to view details of the code resource that it secures.
Delete any privilege by selecting the privilege and clicking the Delete icon.

7. Click Next.

Note: You can add existing privileges to the new role but can’t create new functional security policies.

Adding Data Security Policies

On the Create Role: Data Security Policies page, you can assign data security policies to your new role. For information about creating and adding data security policies to a role, see the topic Editing Data Security Policies on the Security Console.

Click Next to continue to the next page.

Building the Role Hierarchy

The Create Role: Role Hierarchy page shows the hierarchy of your custom role in tabular format by default. You can add one or more job, abstract, and duty roles to the new role. Typically, when creating a job or abstract role you add duty roles. Roles are always added directly to the role that you’re creating.

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 Create Role: Role Hierarchy page shows the updated role hierarchy.
7. Click Next.

Assigning the Role to Users

On the Create Role: Users page, you can assign the job or abstract role you are creating to selected users.

To assign the role to a user:

1. Click Add User.
2. In the Add User dialog box, search for and select a user or role.
3. If you select a role, then click Add Selected Users to add all the users assigned the role to the role you’re creating.
   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 to add additional users.
6. Close the Add User dialog box.
   The Create Role: Users page shows the updated role membership.
7. Click Next.

Reviewing the Role

To review the role, do the following:

1. On the Create Role: Summary and Impact Report page, review the selections you have made.
Summary listings show the numbers of function security policies, data security policies, roles, and users you have added and removed; an Impact listing shows the number of roles and users affected by your changes. Expand any of these listings to see names of policies, roles, or users included in its counts.

2. If you determine you need to make changes, click **Back** to navigate back to the appropriate page, then make the correction.

3. If you’re satisfied with the role, click **Save and Close** to save the role.

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

Your custom role is available immediately on the Security Console.

**Tip:** Search for the job or abstract role on the Security Console and review its visualization. Edit the role to make any corrections.

### Copying and Editing Duty Roles

You can copy a duty role and then edit the copy to create a new duty role. Copying duty roles is the recommended way of creating duty roles. This topic explains how to copy a duty role and edit the copy. You must have the IT Security Manager job role to perform these tasks.

**Copying a Duty Role**

To copy a duty role:

1. On the Roles tab of the Security Console, search for the duty role to copy.
2. Select the role in the search results.
   
   The role is displayed in tabular format by default. Click the Show Graph icon to show the hierarchy in graphical format.
3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
   
   - If you select **Copy top role**, then only the selected role is copied. The copied role inherits the same role instances as the source role.
   - If you select **Copy top role and inherited roles**, then a copy is made of every role in the role hierarchy provided that a copy of the role with the same name doesn’t already exist.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   **Tip:** The **Role Name** and **Role Code** values are assigned the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. The prefix **ORA_** is also removed from the role code. You can overwrite the default prefix and suffix for the role that you’re copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is Complete, you can edit the copied role.

Editing the Copied Duty Role

To edit the copied role, perform the following steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty 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.
4. Click Next.

Managing Functional Security Policies

On the Edit Role: Function Security Policies page, any functional 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 duty roles but can’t create new functional security policies. To delete a privilege that is 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 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 Privilege to grant 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.
    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. As you can’t grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can’t edit these values.

Managing Data Security Policies

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

Click Next to continue to the next page.

Adding and Removing Inherited Roles

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles that it inherits. The hierarchy is displayed in tabular format by default. 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 information message.

To add a role:

1. Click Add Role.
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.

Viewing Users Assigned the Role
On the Edit Role: Users page, click Next. You can’t provision duty roles directly to users.

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

1. Click Back to make corrections.
2. When you have 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.

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

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

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

1. On the Data Security Policies page, locate the policy then click the down arrow at the end of the policy row to show the actions menu.
2. Select one of the options listed:
   o To remove the policy, select the Remove Data Security Policy option.
     The policy is removed from the role.
   o To edit the policy, do the following:
     i. Select the Edit Data Security Policy option.
The **Edit Data Security Policy** dialog box is displayed.

- ii. Change the values as required, for example, you can change the start date, the data set, or the action specified for the policy.
- iii. Click **OK** to save your changes, and close the confirmation message.

### Creating Data Security Policies for Roles

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

To create a data security policy:

1. On the Data Security Policies page, click **Create Data Security Policy**.

   The **Create Data Security Policy** dialog box is displayed. A **Start Date** value is automatically assigned to the policy but can be changed.

2. In the **Policy Name** field, enter a policy name.

   The names of predefined data security policies begin with the words **Grant on**.

3. Search for and select the database resource for which you're defining the policy, for example, search for a table name.

4. In the **Data Set** field, select the subset of the data made available by the database resource the policy applies to.

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

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select by key</td>
<td>Use to limit the data set to a single record in the data resource. If you select this option, you must specify the primary key value that identifies the record in the database resource.</td>
</tr>
<tr>
<td>Select by instance set</td>
<td>Use to limit the data set to a subset of the data in the data resource. If you select this option, you must select a condition that defines a subset of the data. Conditions vary by resource.</td>
</tr>
</tbody>
</table>

   If the predefined conditions available for a resource are not appropriate, you can create custom conditions for the predefined database resource. For additional information, see the topic **Managing Database Resources**.

| All values            | Use to include all data from the data resource in the data set.                                                                                   |

5. Complete the remaining fields, which depend on the selected combination of database resource and data set values.

6. In the **Actions** field, select the actions to which this data security policy applies.

7. Click **OK** to save the data security policy.

You can view the new policy on the Data Security Policies page by scrolling to the end of the list of policies.
Chapter 14
Reviewing and Configuring Data Security

Configuring Data Security: Overview

This chapter describes some of the ways in which you can configure data security for sales and service users.

The database resources of an enterprise are secured using data security policies, which specify the roles that can perform a specified action on an object, and the conditions under which the action can be carried out. The conditions specified in data security policies control visibility to record-level sales and service data associated with a schema object, such as an opportunity. Conditions can use a number of components, such as team or territory access, as mechanisms for sharing data.

For example, a user assigned a role that grants access to opportunities based on team and territory can access the opportunity as part of territory visibility even though the user is not on the opportunity team. The scope of visibility varies by object and multiple visibility levels are supported by an object for a role.

Sales and Service Access Management Work Area

IT Security administrators need to be able to easily view the set of data a predefined role has access to and to easily configure access to a set of data for a user group using custom roles. Both tasks can be performed using the Sales and Service Access Management work area, which provides a simple interface where you can:

- View data access by object for a predefined or custom role.
- Configure data security to add or remove a role’s access to object data.
- End-date policies and configure advanced data permissions.
- Extend access to additional objects for custom roles.

It is recommended that you use the Sales and Service Access Management work area to review and configure data security. However, there are a number of data security configuration tasks you can only do in the Security Console, for example, creating database resources and defining custom conditions for a resource. Data security changes made in either work area are immediately available in both work areas.

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

Access to the Sales and Service Access Management Work Area

The Manage Sales and Service Access privilege (ZCA_MANAGE_SALES_AND_SERVICE_ACCESS_PRIV) grants access to the Sales and Service Access Management work area. This privilege is assigned by default to the IT Security Manager and the Customer Relationship Management Application Administrator job roles. If necessary, you can provide access to the work area by granting the Manage Sales and Service Access functional privilege to a custom job role.
Reviewing Data Access for a Role and Object

You can review the visibility provided by job roles to object data on the main Sales and Service Access Management page. This page displays a read-only view of all the data security policies provided by a predefined or custom role for an object. You can use this information to query existing policies so you can determine, for example:

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

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

Perform the steps in the following procedure to review data access for a selected role and object:

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.

2. Select **Navigator > Tools > Sales and Service Access Management**.

   The Sales and Service Access Management page is displayed. It contains two areas: the Access Policies table, which lists each data policy for the selected object and role combination, and the Advanced Permissions table, which shows more detail about any advanced permissions available for a policy selected in the Access Policies table.

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

3. Search for or select a role in the **Role** field.

   You can select either a custom or a predefined role. For example, to search for the Sales Representative role:

   a. In the **Role** field drop-down list, click **Search**, then enter the role name in the **Role** field of the Role dialog box.

   b. Click **Search** again. From the search results, select the role you want, then click **OK**. Note that in the search results predefined roles are identified by a **Yes** in the Predefined role column.

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

   The **Object** field lists all the sales and service objects for which the role has been granted access permissions. For example, select the **Opportunity** object.

   The Access Policies table is now populated with a list of all the active data security policies relating to opportunities for the selected role. You can view more or less information for the policies in the table by selecting the **Columns** option in the **View** menu.

   The following table shows the information available for each active policy in the Access Policies table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Lists the condition under which this data policy takes effect. For example, if you selected the Sales Representative role and the Opportunity object, the condition might state that this policy applies when the user assigned the Sales Representative role is an opportunity sales team member with edit or full access.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permissions</td>
<td>The Read, Update, and Delete Permissions columns show the access provided by the policy. For example, if all three actions are selected, then this policy provides a user with read, update, and delete access to the object when the conditions specified in the criteria are met, for example, the user is an opportunity sales team member with edit or full access.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Indicates how many advanced permissions exist (if any) for this policy. Advanced permissions provide a finer grained method of controlling what the user can do. For example, a policy might provide update access to an opportunity but the Advanced Permission allows you to restrict that update access to specific attributes. Not all objects or policies have advanced permissions.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Indicates the date on which the policy was activated.</td>
</tr>
<tr>
<td>End Date</td>
<td>Indicates the date on which the policy is deactivated.</td>
</tr>
<tr>
<td>Role</td>
<td>Lists the name of the role the policy is associated with. In most cases, the policy relates to the top-level job role you selected in the Role column, but in some cases, the policy is provided by an inherited duty role.</td>
</tr>
<tr>
<td>Custom Criteria</td>
<td>Indicates whether the condition specified in the policy is a predefined condition provided by Oracle or is a custom condition that you created previously.</td>
</tr>
</tbody>
</table>

5. If you want to view the inactive policies for the selected role and object in the Access Policies table, select the Inactive policies check box.

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

Edithing the Data Access Permissions for a Custom Role and an Object

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

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

The following procedure describes how to edit the data security permissions to object data for a custom role.

To edit security permissions:

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

3. Search for or select a role in the **Role** field.
   You cannot edit policies on predefined roles, so search for and select a custom role. For example, if you copied the predefined Sales Representative role to create a custom version of the role, you could select it.

4. Select an object in the **Object** field, for example, select the **Sales Lead** object.

5. Click the **Edit** icon and the Active Policies edit page for the selected role and object is displayed.
   The Access Policies table shows policies that provide existing data grants, future-dated data grants, available instance sets that aren’t yet granted, and global records (All records).

6. Configure the access provided to the selected object for the selected custom role by selecting or deselecting the **Read**, **Update**, or **Delete** check boxes for a policy.
   For example, if you are editing policies for a custom Sales Representative role and the Sales Lead object, you can perform data configuration tasks such as:
   - Restrict the ability to delete leads to lead owners by locating any policies that provide lead access to team members and deselecting the **Delete** check box for these policies.
   - Allow sales representatives to view retired leads by locating the policy that grants this access, then clicking the **Read** check box.

   ✏️ **Note:** For each policy in the Access Policies table, the **Role** field lists the role that the policy is associated with; this is either the top-level job role you selected, or an inherited duty role. You can’t configure policies that are inherited from predefined duty roles as predefined roles can’t be edited.

7. You can remove all access granted by a policy. For example, if your company does not use territory access, you can remove territory access to lead data using one of the following methods:
   - Review the Criteria column to locate the policies that grant territory access, then deselect the **Read**, **Update** and **Delete** check boxes for each of these policies.
   - End-date the policies so that they are no longer active by selecting a date that has passed in the **End Date** field, for example, select yesterday’s date.

   ✏️ **Note:** To reactivate a policy that is deactivated, reassign the appropriate read, update, and delete permissions to the relevant criteria and specify a start date for the policy.

8. If a policy has an advanced permission associated with it, then you can edit the advanced permission to specify more granular levels of access to the object.
   For example, a policy might provide full access to lead data for a resource in the territory assigned to the sales lead. You can restrict this access by selecting the policy, then scrolling to the Advanced Permissions table for the policy.
   You can remove update access to the lead data but retain read access by deselecting the **Update** check boxes.

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

9. Click **Save and Close**.
   Your changes are saved and the Sales and Service Access Management page is displayed where you can review your changes. If you have end-dated a policy, note that the number in parentheses beside the **Inactive policies** check box is incremented.
Editing Inactive Policies

If you specified an end date for a policy, then once the end date is passed, the policy is inactive. You cannot edit inactive policies for custom roles but you can delete them, as described in the following procedure.

To delete an inactive policy:

1. On the Sales and Service Access Management page, select a custom role in the Role field and an object in the Object field.
2. Click the Inactive policies check box.
3. Click the Edit icon.
4. On the Inactive Policies page, select a policy and click the Delete icon.
5. Click Yes when a warning is displayed.
6. Click Save and Close to return to the main page.

The deleted policy is no longer included in the Access Policies list and the number in parentheses beside the Inactive policies check box is reduced.

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

Extending Access to Additional Objects for a Custom Role

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

For example, if you want to provide sales managers with access to budget data for a specific initiative, then you have to create access to the relevant budget object for a custom version of the Sales Manager job role, because the Sales Manager job role doesn’t provide access to budget data by default. The following procedure describes how to create access to a new object for a custom role.

To extend object access for a role:

1. On the Sales and Service Access Management page, search for the custom role whose access you want to extend in the Role field.
2. Click the Create button.
3. On the Create Policies page, select the object you want to provide access to in the Object field.

   For example, select the object for budgets, MDF Budget. The only objects available for selection are objects where data security policies are not already defined for the custom role.

   All the data security policies defined for the selected object are displayed in the Access Policies table. There are no permissions selected in the Permissions columns because data access to the object hasn’t previously been configured for the custom role you selected.

4. Locate the criteria that provides the data access you want to implement for the object.
For example, if you want to provide the custom sales manager role with read access to all budgets that have a status of Draft up to the end of the year, then do the following:

a. Locate the condition that provides the required access. For example, locate a condition similar to the following: *Access the MDF budget for table MKT_BDT_BUDGETS_B for all MDF budgets in the enterprise, and the MDF budget is in draft status.*

b. Click the **Read** check box for this condition.

c. Specify a **Start Date** of today and an appropriate **End Date**.

5. Click **Save and Close**.

On the Sales and Service Access Management page, the new policies you have added are now listed in the Access Policies table.

\[\text{Note:}\] You can view data security for custom objects using the Sales and Service Access Management work area, but you can only edit security policies for custom objects using Application Composer.

### Managing Database Resources

Data security policies secure the database resources of an enterprise. This topic describes how to manage database resources and data security policies if, for example, you want to define and secure a new database resource, or if the predefined data security conditions for a database resource don’t meet your needs. Using the Manage Database Resources and Policies page of the Security Console, you can:

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

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

### Defining Database Resources

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

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

The following procedure describes each of these tasks.

To define a new database resource:

1. On the Security Console Administration tab, select the General subtab, then click **Manage Database Resources**. The Manage Database Resources and Policies page is displayed.
2. In the Search Results region, click the Create icon.

The Create Database Resource page is displayed. The General Information subtab is selected by default.

3. Enter the values for the new database resource.

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

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

4. Click the Function Security Enabled check box if functional security policies have been defined for the business object.

5. In the Primary Key Columns area, click the Create icon.

6. In the Primary Key field, select the primary key column of the database table or view that the business object represents.

7. In the Filter Column Details area, select columns you want to exclude from the row instance sets defined by data security policies. The data from filtered columns isn’t accessible by users. To select a column as a data filter, move it from the Available Columns list to the Selected Columns list.

8. Click the Condition subtab to create conditions for the new database resource, then click the Create icon.

The Create Database Resource Condition dialog box is displayed. Conditions specify the rows of the database resource that can be secured by data security policies.

9. Create resource conditions as described in the procedure Creating Conditions for a Database Resource later in this topic.

10. Click the Action subtab.

You define actions on the database resource to specify the operations data security policies can secure on a business object. For example, you can specify whether a user might have read, update, or delete access by naming actions for each of these and granting them in a data security policy to a particular role. An action must correspond with an operation that the business object implements.

11. Click the Add Row icon.

12. Enter a value in the Name and Display Name fields. The action name you enter must match an operation name defined for the corresponding business object. Actions act on the row instance sets specified by the database resource conditions that you define in a data security policy, that is, conditions determine the row instance set available to a user for a given action.

You can specify more than one action.

13. Click Submit.

14. When the confirmation dialog box is displayed confirming that the database resource was created, click OK.
Creating Conditions for a Database Resource

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

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

To create conditions for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources. The Manage Database Resources and Policies page is displayed.
2. Search for the database resource whose conditions you want to edit.
3. In the Search Results list, select the appropriate database resource, then click the Edit icon. The Edit Data Security page is displayed.
4. Select the Condition subtab to define a new condition for the resource. Any existing conditions defined for the database resource are displayed. You can’t delete or edit any predefined conditions.
5. Click the Create icon. The Create Database Resource Condition dialog box is displayed.
6. Enter a name and display name for the condition.
7. For the Condition Type, select one of the following:
   - Select Filter if you want to use the attribute picker to define a simple condition. If you select the filter condition type, you also must specify the following values:
     - For the Match option, select the All option if you want the filter conditions to include AND clauses or select the Any option if you want the filter conditions to include OR clauses.
     - In the Conditions area, click the Add icon.
     - Define the filter values.

The following table describes the filter values for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column Name</td>
<td>Select the column for which you’re defining the filter.</td>
</tr>
<tr>
<td>Tree Operators</td>
<td>Select this option if the operator you want to use in the filter is a tree operator.</td>
</tr>
<tr>
<td>Operator</td>
<td>Choose the operator for the selected column filter.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value as the test for the operator.</td>
</tr>
</tbody>
</table>
If you specified the Tree Operators option, click the Search icon. The Select Tree Node dialog box is displayed allowing you to choose the operator value.

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

  8. Click Save to save the new condition.

Create a Data Security Policy for a Database Resource

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

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

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

To create a policy for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.
   
   The Manage Database Resources and Policies page is displayed.
2. Search for the database resource that you want to secure by defining a policy.
3. In the Search Results list, select the database resource, then scroll down to the Policies Details area.
   
   All the policies defined for the database resource are displayed.
4. You can select an existing policy for editing by selecting the policy then clicking the Edit icon. In this case, however, click the Create icon to create a new policy.
   
   The Create Policy dialog box is displayed with the General subtab selected.
5. Specify the following information for the new policy:
   
   - In the Name field, enter a name for the policy.
   - In the Start Date field, enter the date on which the policy is to become active.

   The Module field is pre-filled with the name of the module associated with the database resource for which you’re creating the policy but you can change this value.
6. Click the Role subtab, then click the Add icon to select the roles that are to be assigned the new policy.
   
   The Select and Add: Roles dialog box is displayed.
7. Select the roles to be assigned the new policy as follows:
   
   - In the Role Name field, enter the name of the role.
   - In the Application field, enter the application stripe of the role, for example, CRM, HCM, or FSCM, then click Search.
Select a role from the list of roles displayed, then click **Apply** to associate the role with the new policy.

Select any additional roles from the list and, when you have finished adding roles, click **OK**.

All users assigned the roles you select are provided with access to the data defined in the policy.

8. Click the Rule subtab to define a rule to specify the rows of the database resource to which the policy applies.

9. Select one of the following values in the **Row Set** field:

   - To secure a specific row, select **Single Value**, then search for and select the row you want to secure in the **Row** field.
   - To secure all rows in the resource, select **All Values**.
   - To secure a subset of the data in the data resource select **Multiple Values**, then search for and select the condition that defines the subset of the data to be secured in the **Condition** field.

10. Click the Action subtab, then move actions from the Available Actions list to the Selected Actions list to specify the actions, applicable to the data secured on the database resource, which you want to grant to the role.

11. Click **Save and Close**.
15 Security and Reporting

Security for Sales Cloud Analytics and Reports

Analytics are available throughout the sales application as embedded analytics and also in standalone mode by way of the transactional work areas. Sales users interact with information in Oracle BI Applications and Oracle Transactional Business Intelligence using Oracle Business Intelligence Enterprise Edition (Oracle BI EE) components, such as Dashboards.

The analytics and reports that are delivered with the sales application are secured based on the roles that use each report. For example, sales managers can access sales analytics and reports that salespeople don't have access to. If you want to create new analytics or reports or edit existing ones, you should become familiar with sales security concepts and how access is secured to Oracle Transactional Business Intelligence subject areas, Oracle BI Presentation Catalog folders, and Oracle Business Intelligence reports.

Subject Areas

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

Business Intelligence Catalog Folders

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

Business Intelligence Reports

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

Information about Security and Reporting

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

- Oracle Sales Cloud Security Reference
Describes the sales application security reference implementation and includes descriptions of all the predefined data that is included in the security reference implementation for an offering.

- Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition

Provides information about using Transactional Analysis Duty roles to secure access to the Business Intelligence catalog.

- Creating and Administering Analytics for Sales

Explains how to view and work with analytics and reports.

Permissions for Catalog Objects

The Business Intelligence Catalog stores business intelligence objects such as dashboards, dashboard pages, folders, and analyses. Users can view only the objects for which they are authorized. Note that the owner of an object or folder cannot automatically access the object or folder. To access an object or folder, the user must have the proper permission assigned in the object or folder’s permission dialog.

What Are Permissions?

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

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

Permission Definitions

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

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

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>Use this option to give authority to perform all tasks (modify and delete, for example) on the object.</td>
</tr>
<tr>
<td>Modify</td>
<td>Use this option to give authority to read, write, and delete the object.</td>
</tr>
</tbody>
</table>
### Permission | Definition
--- | ---
Traverse | Use this option to give authority to access objects within the selected folder when the user does not have permission to the selected folder. Access to these objects is required when the objects in the folder, such as analyses, are embedded in a dashboard or Oracle WebCenter Portal application page that the user has permission to access.

For example, if you grant users the Traverse permission to the /Shared Folders/Test folder, then they can access objects, through the BI Presentation Catalog or embedded in dashboards or Oracle WebCenter Portal application pages, stored in the /Shared Folders/Test folder and stored in sub-folders, such as the /Shared Folders/Test/Guest folder. However, users cannot access (meaning view, expand, or browse) the folder and sub-folders from the Catalog.

Open | Use this option to give authority to access, but not modify, the object. If you are working with an Oracle BI Publisher object, this option enables you to traverse the folder that contains the object.

No Access | Use this option to deny access to the object. Explicitly denying access takes precedence over any other permission.

Custom | Use this option to display the Custom Permissions dialog, where you grant read, write, execute, and delete permissions.

For additional information about catalog object permissions, see Oracle Fusion Middleware User’s Guide for Oracle Business Intelligence Enterprise Edition on Oracle Help Center at [http://docs.oracle.com/](http://docs.oracle.com/).

### Transaction Analysis Duty Roles

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

Your administrator can select users, roles, and catalog groups to:

- Receive the delivery content of an agent.
- Have permission to access a section or alert section in a dashboard.
- Add or edit for an existing catalog group.
- Assign permissions to a catalog object.

For information about setting the necessary security, see Oracle Middleware Security Guide for Oracle Business Intelligence Enterprise Edition.

The following is a list of some OTBI Transactional Analysis Duty roles used in the sales application:

- Partner Channel Transaction Analysis Duty
- Partner Channel Administrative Transaction Analysis Duty
- Sales Administrative Transaction Analysis Duty
- Sales Executive Transaction Analysis Duty
- Sales Managerial Transaction Analysis Duty
- Sales Transaction Analysis Duty
The following table lists analytics and reports available to sales users. It also shows the predefined job roles that can access the different analytics and reports, and the OTBI Transactional Analysis Duty roles that provide the access.

<table>
<thead>
<tr>
<th>Analytic or Report Name</th>
<th>Job Role</th>
<th>OTBI Transactional Analysis Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Forecast vs. Quota</td>
<td>Sales VP</td>
<td>Sales Executive Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Sales Stage by Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Sales Performance Trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Top Open Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Forecast Vs Open Pipeline: My Team</td>
<td>Sales Manager</td>
<td>Sales Managerial Transaction Analysis Duty</td>
</tr>
<tr>
<td>• My Team’s Activities (By Type)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Team’s Leads</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Team’s Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Team’s Pipeline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Team’s Tasks on Open Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Team’s Top Open Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Team Leadership Board</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Top Accounts by My Team’s Activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Open Leads by Age</td>
<td>Sales Representative</td>
<td>Sales Transaction Analysis Duty</td>
</tr>
<tr>
<td>• My Top Open Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Forecast vs. Open Pipeline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Open Leads by Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Open Tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Pipeline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Stalled Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Top Accounts by Open Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Unaccepted Leads by Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Won Opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• My Top Accounts by My Activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Evaluating My Partners’ Pipeline</td>
<td>Channel Account Manager</td>
<td>Partner Channel Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Evaluating My Partners’ Quarterly and Yearly Closed Revenue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Evaluating My Partners’ Current Quarterly Sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Evaluating My Partners’ Win Rate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Business Intelligence Roles**

Business Intelligence roles apply to both Oracle Business Intelligence Publisher (Oracle BI Publisher) and Oracle Transactional Business Intelligence (OTBI). They grant access to Business Intelligence functionality, such as the ability to run or author...
reports. Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and sales data. This topic describes the Business Intelligence roles.

The Business Intelligence roles are described in the following table.

<table>
<thead>
<tr>
<th>Business Intelligence Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI Consumer Role</td>
<td>Runs Business Intelligence reports.</td>
</tr>
<tr>
<td>BI Author Role</td>
<td>Creates and edits reports.</td>
</tr>
<tr>
<td>BI Administrator Role</td>
<td>Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.</td>
</tr>
<tr>
<td>BI Publisher Data Model Developer Role</td>
<td>Creates and edits Oracle Business Intelligence Publisher data models.</td>
</tr>
</tbody>
</table>

**BI Consumer Role**

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

**BI Author Role**

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

**BI Administrator Role**

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role. The predefined sales job roles do not have BI Administrator Role access.

**BI Publisher Data Model Developer Role**

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Therefore, users with either of these predefined job roles can manage BI Publisher data models.
Configuring Security for Oracle Transactional Business Intelligence: Explained

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

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles, for example, Sales Managerial Transaction Analysis Duty. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.

- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports and subject areas to create and run reports and view analytics.

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

Modifying Transaction Analysis Duty Role Assignments

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

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

Modifying Business Intelligence Role Assignments

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

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

All predefined sales job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default, except for the Sales Representative job role. However, you can optionally create copies of the predefined job roles and add or remove the BI Author Role from the custom roles as required.

Viewing Reporting Roles

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

- The reporting roles that a job role inherits
- The reporting roles you are assigned
Viewing the Reporting Roles Assigned to a Job Role

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

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

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

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

Viewing the Reporting Roles You Are Assigned

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

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

   The Business Intelligence Catalog page opens.
3. Click your user name in the global header, then select My Account.
4. Click the Roles and Catalog Groups tab.

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

FAQs for Security and Reporting

Can I configure Oracle Transactional Business Intelligence duty roles?

You can’t modify the predefined OTBI duty roles or the associated security privileges. You can configure Oracle Transactional Business Intelligence reporting security by assigning different OTBI duty roles to a custom job role according to your needs.
16 Security and Personally Identifiable Information

Security and Personally Identifiable Information: Overview

Securing and protecting confidential customer information against data breaches, data theft, or unauthorized access is an increasing concern for enterprises. To address this issue, Oracle restricts access to certain information, known as Personally Identifiable Information (PII), that is considered private to an individual. This chapter describes how personally identifiable information is secured in Oracle Applications Cloud.

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

Protecting Personally Identifiable Information

The data or information that is used to uniquely identify a contact, or locate a person is called personally identifiable information (PII), such as social security number, addresses, bank account numbers, phone numbers, and so on. This information is considered confidential and sensitive, and must be protected to prevent unauthorized use of personal information for the purposes of legal regulation, financial liability, and personal reputation. For example, only authorized users must be allowed access to the social security numbers of people stored in a system.

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

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

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

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

<table>
<thead>
<tr>
<th>PII Attribute</th>
<th>Table Name</th>
<th>Privilege Title</th>
<th>Privilege Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taxpayer Identification Number (Social Security Number)</td>
<td>HZ_PERSON_PROFILES</td>
<td>View Trading Community Person Social Security</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_SOCIAL_SECURITY_DATA</td>
</tr>
<tr>
<td>Taxpayer Identification Number (Social Security Number)</td>
<td>HZ_PERSON_PROFILES</td>
<td>Manage Trading Community Person Social Security</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_SOCIAL_SECURITY_DATA</td>
</tr>
<tr>
<td>PII Attribute</td>
<td>Table Name</td>
<td>Privilege Title</td>
<td>Privilege Name</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Citizenship Number</td>
<td>HZ_CITIZENSHIP</td>
<td>View Trading Community Person Citizenship Number</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_CITIZENSHIP_NUMBER_DATA</td>
</tr>
<tr>
<td>Citizenship Number</td>
<td>HZ_CITIZENSHIP</td>
<td>Manage Trading Community Person Citizenship Number</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_CITIZENSHIP_NUMBER_DATA</td>
</tr>
<tr>
<td>Home Address</td>
<td>HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITEUSES table</td>
<td>View Trading Community Person Address</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_ADDRESS_DATA</td>
</tr>
<tr>
<td>Home Address</td>
<td>HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITEUSES table</td>
<td>Manage Trading Community Person Address</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_ADDRESS_DATA</td>
</tr>
<tr>
<td>Home Phone</td>
<td>HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL</td>
<td>View Trading Community Person Contact</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_CONTACT_DATA</td>
</tr>
<tr>
<td>Home Phone</td>
<td>HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL</td>
<td>Manage Trading Community Person Contact</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_CONTACT_DATA</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE</td>
<td>View Trading Community Person Mobile Phone Number</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_MOBILE_PHONE_DATA</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE</td>
<td>Manage Trading Community Person Mobile Phone Number</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_MOBILE_PHONE_DATA</td>
</tr>
<tr>
<td>Home Email</td>
<td>HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL</td>
<td>View Trading Community Person Contact</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_CONTACT_DATA</td>
</tr>
<tr>
<td>Home Email</td>
<td>HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL</td>
<td>Manage Trading Community Person Contact</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_CONTACT_DATA</td>
</tr>
<tr>
<td>Additional Identifiers</td>
<td>All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS</td>
<td>View Trading Community Person Additional Identifier</td>
<td>HZ_VIEW_TRADING_COMMUNITY_PERSON_ADDITIONAL_IDENTIFIER_DATA</td>
</tr>
<tr>
<td>Additional Identifiers</td>
<td>All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS</td>
<td>Manage Trading Community Person Additional Identifier</td>
<td>HZ_MANAGE_TRADING_COMMUNITY_PERSON_ADDITIONAL_IDENTIFIER_DATA</td>
</tr>
</tbody>
</table>
Role Optimization

Role Optimizer Overview

Role optimization is the process used to analyze the existing role hierarchy for redundancies or other inefficiencies. Role optimization enables you to create a role hierarchy that minimizes the number of roles necessary to authorize every job role to its currently authorized privileges. The role optimizer feature automates the analysis process and generates a report you can use to optimize your job hierarchies.

Reasons to Optimize

Changes to the predefined role hierarchies can put the privacy of your application data at risk. You can unintentionally make your data less secure if you:

- Create duty roles with small groups of privileges in an attempt to minimize:
  - Dependencies
  - The impact of making incremental changes
- Grant privileges that already exist in the role hierarchy

The following figure shows how roles can proliferate or have duplicate privileges over time making your role hierarchy less efficient.
Benefits of Optimization

By using the role optimizer, you can:

- Increase user productivity.
  
  You save time that you can perform other tasks.

- Reduce administrative costs.
  
  You reduce the number of security objects and the amount of time you spend maintaining that you must administer them.

- Decrease access risk associated with undocumented role hierarchy changes.
  
  You identify and can eliminate redundant and inappropriate grants of privilege.

The following figure shows how the role optimizer can suggest more efficient role hierarchies.

Role Optimizer Access

The role optimizer feature is available as a predefined report. Schedule and submit the Role Optimization Report on the Overview page of the Scheduled Processes work area. The process:

1. Analyzes your existing job role hierarchies.
2. Generates the optimized job role hierarchy and stores the data for each job role in a separate CSV file.
3. Archives and attaches the CSV files as the process output.
4. Generates a log and archives it as a ZIP file. The log file includes technical details of the analysis for troubleshooting.
Note: The role optimization process makes no changes to your security structures. You use the report to map privileges to roles and update the role hierarchies.

Role Optimization Report

Use the Role Optimization Report to create the most efficient role hierarchy for your organization. Use the report results to evaluate and, if necessary, update your role hierarchy. The report results enable you to create a role hierarchy with the minimum number of roles necessary to authorize every job role to every privilege it is currently authorized to.

Users with the IT Security Manager role can run the Role Optimization Report, which is available from the security console.

You should run this report if you:

- Make changes to the predefined role hierarchy.
- Implement your own role hierarchy instead of the predefined role hierarchy.

Note: The process makes no changes to your role hierarchies.

The predefined role hierarchy in the security reference implementation is optimized as delivered.

Report Files

Monitor the process status on the Overview page. When the status value is Succeeded, two files appear in the Log and Output section of the report details.

The following table describes the two files that appear when you run the Role Optimization report.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterAnalysis-Job-CSVs.zip</td>
<td>Contains one CSV file for every job role. Each CSV file contains the duty roles and privileges that make up the optimized job role hierarchy. The name of a CSV file, identifies the job role hierarchy data that the file contains. For example, the ClustersforJob-AR_REVENUE_MANAGER_JOB_14240.csv file contains all of the role hierarchy data for the Accounts Receivables Revenue Manager job role.</td>
</tr>
<tr>
<td>Diagnostics. zip</td>
<td>Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.</td>
</tr>
</tbody>
</table>

Import the raw data from the CSV file into your preferred application to read the results. Report data appears in these two sections:

- Privilege Clusters
- Cluster Details
Role Optimization Report Results

Privilege Clusters
The Privilege Clusters section lists each privilege and the name of a recommended privilege cluster. Specific cluster recommendations are described in the cluster details section.

Cluster Details
A Cluster Details section appears for each privilege cluster referenced in the Privilege Clusters section. Each detail section includes:

- Cluster name.
- Names of recommended candidate roles that map to the privilege cluster.
- Names and descriptions of the jobs and privileges associated with the cluster.

The following table provides descriptions of the fields that appear in the Cluster Details section.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The name of the optimized cluster, usually in this format: Cluster ###</td>
</tr>
<tr>
<td>Primary, Secondary, Tertiary Candidate Role</td>
<td>Recommended role mappings for the privileges in the cluster. Up to three recommended duty roles map to the listed privileges. Select a role. Then assign the privileges in the cluster to that role.</td>
</tr>
<tr>
<td>Jobs in Cluster</td>
<td>The number of job roles that inherit the privilege cluster. A list of job names and descriptions is also included.</td>
</tr>
<tr>
<td>Privileges in Cluster</td>
<td>The number of privileges that make up the cluster. A list of privilege names and descriptions is also included.</td>
</tr>
</tbody>
</table>
18 Advanced Data Security

Advanced Data Security offers two types of added data protection. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest. Advanced Data Security is available for Oracle Applications Cloud by subscription to Break-Glass service.

Oracle Database Vault
Database Vault reduces the risk of highly privileged users such as database and system administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects.

Administrators can perform regular database maintenance activities, but cannot select from the application tables. If a DBA requires access to the application tables, request temporary access to the Oracle Fusion schema at which point keystroke auditing is enabled.

Transparent Data Encryption
Transparent Data Encryption (TDE) protects Oracle Fusion Applications data which is at rest on the file system from being read or used. Data in the database files (DBF) is protected because DBF files are encrypted. Data in backups and in temporary files is protected. All data from an encrypted tablespace is automatically encrypted when written to the undo tablespace, to the redo logs, and to any temporary tablespace.

Advanced security enables encryption at the tablespace level on all tablespaces which contain applications data. This includes SOA tablespaces which might contain dehydrated payloads with applications data.

Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL). Tablespace keys are stored in the header of the tablespace and in the header of each operating system (OS) file that makes up the tablespace. These keys are encrypted with the master key which is stored in the Oracle Wallet. Tablespace keys are AES128-bit encryption while the TDE master key is always an AES256-bit encryption.
Glossary

**abstract role**
A description of a person’s function in the enterprise that is unrelated to the person’s job (position), such as employee, contingent worker, or line manager.

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

**aggregate privilege**
A predefined role that combines one function security privilege with related data security policies.

**assignment**
A set of information, including job, position, pay, compensation, managers, working hours, and work location, that defines a worker’s or nonworker’s role in a legal employer.

**data security**
The control of access and action a user can take against which data.

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

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

**entitlement**
Grant of access to functions and data. Oracle Fusion Middleware term for privilege.

**function security**
The control of access to a page or a specific use of a page. Function security controls what a user can do.

**job**
A generic role that is independent of any single department or location. For example, the jobs Manager and Consultant can occur in many departments.

**job role**
A role, such as an accounts payable manager or application implementation consultant, that usually identifies and aggregates the duties or responsibilities that make up the job.
**LDAP**

**privilege cluster**
In the output of the Role Optimization Report, a group of privileges that you can map to a duty role.

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

**role**
Controls access to application functions and data.

**role hierarchy**
Structure of roles to reflect an organization's lines of authority and responsibility. In a role hierarchy, a parent role inherits all the entitlement of one or more child roles.

**role mapping**
A relationship between one or more roles and one or more assignment conditions. Users with at least one assignment that matches the conditions qualify for the associated roles.

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

**security reference implementation**
Predefined function and data security that includes role based access control, and policies that protect functions, and data. The reference implementation supports identity management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

**setup user**
A user provisioned with the job roles and abstract roles required to perform implementation tasks.

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

**workflow**
An automated process that passes a task from one user (or group of users) to another to view or act on. The task is routed in a logical sequence to achieve an end result.