## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></td>
<td>i</td>
</tr>
<tr>
<td><strong>1 About This Guide</strong></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><strong>2 Authentication</strong></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><strong>3 Authorization with Role-Based Access Control</strong></td>
<td>5</td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td>5</td>
</tr>
<tr>
<td>Predefined Sales and Service Roles</td>
<td>5</td>
</tr>
<tr>
<td>Roles for Workflow Administration Access</td>
<td>7</td>
</tr>
<tr>
<td>Role Types</td>
<td>8</td>
</tr>
<tr>
<td>Role Hierarchies and Role Inheritance</td>
<td>9</td>
</tr>
<tr>
<td>Duty Role Components</td>
<td>10</td>
</tr>
<tr>
<td>Guidelines for Configuring Security</td>
<td>11</td>
</tr>
<tr>
<td>Options for Reviewing Predefined Roles</td>
<td>12</td>
</tr>
<tr>
<td>Oracle Cloud Applications Security Console</td>
<td>13</td>
</tr>
<tr>
<td><strong>4 Data Sharing Mechanisms and Object Visibility</strong></td>
<td>15</td>
</tr>
<tr>
<td>Data Sharing Mechanisms</td>
<td>15</td>
</tr>
<tr>
<td>How Sales 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 for Sales Objects</td>
<td>18</td>
</tr>
<tr>
<td>Data Sharing and Visibility in Incentive Compensation</td>
<td>20</td>
</tr>
<tr>
<td>Data Sharing and Visibility in Service</td>
<td>21</td>
</tr>
</tbody>
</table>
5 **Set Up Applications Security**

- Overview of Applications Security Setup Tasks 23
- Import Users and Roles into Applications Security 23
- Synchronize User and Role Information 24
- Application Security Preferences 24
- Set the Default User-Name Format 25
- Password Policy 26
- Role Preferences 28
- Overview of User Categories 29
- Add Users to a User Category 30
- User-Name and Password Notifications 31
- Create a Notification Template 33
- Schedule the Import User and Role Application Security Data Process 35
- Schedule the Import User Login History Process 36
- Why you Run the Send Pending LDAP Requests Process 36
- Schedule the Send Pending LDAP Requests Process 37
- Give Users the Permission to View All Scheduled Processes 38

6 **Bridge for Microsoft Active Directory**

- Overview 41
- Active Directory Synchronization 42
- User Account Attribute Mapping 43
- Microsoft Active Directory Bridge Setup 44
- FAQs on Working with the Bridge for Microsoft Active Directory 50

7 **Location Based Access**

- Overview 53
- How Location-Based Access Works 53
- Enable and Disable Location-Based Access 54
- FAQs for Location Based Access 55

8 **Single Sign-On**

- Oracle Applications Cloud as the Single Sign-On Service Provider 59
- Configure Single Sign-On 59
- FAQs on Single Sign-On 61
9 API Authentication 65
Configure Outbound API Authentication Using JWT Custom Claims 65
Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol 65
Configure Inbound Authentication 67
Is there a recommended format for the public certificate? 68

10 Export and Import of Security Setup Data 69
Export and Import of Security Console Data 69
Export and Import of HCM Custom Roles and Security Profiles 70

11 Sales Users and Role Provisioning 81
Types of Sales Users 81
Methods of Creating Sales Users 83
Tasks You Accomplish by Creating Users 84
Role Provisioning 85
Steps for Setting Up Role Provisioning 91

12 Get Ready to Create Sales Users 93
What You Must Do Before Creating Sales Users 93
Create a Resource Organization 94
Designate an Organization as the Top of the Sales Hierarchy 95
Prevent Entry of Duplicate User Email Addresses 96
Create Additional Resource Roles 97
Create Rules to Automatically Provision Job Roles to Sales Users 97
Define Rules for Incentive Compensation Abstract Roles 99
Role Provisioning Options 100
Role Autoprovisioning 102
Provision Roles for Testing 103
FAQs for Preparing for Application Users 105

13 Create Sales Users 107
User Setup Options 107
Create Application Users 107
Create Sales Restricted Users 110
Configure Administrators to Access Incentive Compensation 111
14 User Management

Overview of Managing Users
Reset Passwords for Other Users
Change a User's Email Address
Get User Sign-in Sign-out Information
Change User Names
Change User Resource Roles When Job Assignments Change
View Locked Users and Unlock Users
Terminate User Accounts
Impersonation and Proxy Users
Provide Read-Only Access for Individual Users
FAQs for Managing Users

15 User and Role Reports

User and Role Access Audit Report
User Role Membership Report
User Password Changes Audit Report
Inactive Users Report
User History Report

16 Review and Analyze Roles

Overview of Reviewing Roles
Graphical and Tabular Role Visualizations
Review Role Hierarchies
Simulate Navigator Menus
Review Role Assignments
Compare Roles
Compare Users
Analytics for Roles
Analytics for Database Resources
View Role Information Using Security Dashboard
## 17 Create and Edit Job, Abstract, and Duty Roles

- Overview of Security Configuration  
- Guidelines for Copying Roles  
- Copy Job or Abstract Roles  
- Edit Job or Abstract Roles  
- Create Job or Abstract Roles  
- Copy and Edit Duty Roles  
- Edit Data Security Policies on the Security Console

## 18 Configure and Troubleshoot Data Security

- Overview of Data Security Configuration  
- Sales and Service Access Management Work Area  
- Review and Configure Data Access for Roles  
- Review and Troubleshoot Data Access Issues for Users  
- Manage Database Resources

## 19 Access Groups

- Overview of Access Groups  
- How Access Groups Work with Other Security Mechanisms  
- Considerations in Deciding When to Use Access Groups  
- Types of Access Groups  
- Overview of the Access Groups UI  
- Create and Manage Custom Access Groups  
- Add Members to Custom Access Groups  
- Manage System Access Groups  
- Manage Object Sharing Rules for Access Groups  
- Assign Group Access By Country  
- Import and Export Access Groups, Members, and Rules  
- How Data Security Policies Map to Access Group Predefined Rules
20 Security and Reporting

- Security for Sales Analytics and Reports 241
- Permissions for Catalog Objects 242
- Transaction Analysis Duty Roles 243
- Business Intelligence Roles 244
- Configure Security for Oracle Transactional Business Intelligence 246
- View Reporting Roles 246
- Display Direct Report Data in Participant Manager Reports 247
- FAQs for Security and Reporting 248

21 Security and Personally Identifiable Information

- Overview 251
- How to Protect Personally Identifiable Information 251

22 Advanced Data Security

- Advanced Data Security 255
Preface

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

Using Oracle 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 the Oracle Help Center to find guides and videos.

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

You can also read about it instead.

Additional Resources

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

- **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>boldface</td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td>monospace</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.
1 About This Guide

Audience and Scope

This guide provides you with the concepts and procedures you need to implement and administer security. You perform some of the tasks described in this guide only when you're implementing the sales applications. But most tasks can be performed at any time and as new requirements emerge. Use the guide to learn more about topics such as these:

- How role-based access control is implemented in the sales applications.
- 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 and the Sales and Service Access Management work areas.
- How to create security artifacts, such as security policies and roles.

During implementation, you perform security-related tasks from a functional area task list. Once the implementation is complete, you can perform most security-related tasks on the Security Console or the Sales and Service Access Management work area. 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

Refer to the following guides for additional information about implementing and administering Oracle CX Sales and B2B Service.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle CX Sales Getting Started with Your Sales Implementation</td>
<td>Describes the initial procedures for implementing Oracle CX Sales using a simple, sales-automation use case.</td>
</tr>
<tr>
<td>Oracle CX Sales Implementing Sales</td>
<td>Contains conceptual information and procedures for implementing the components and features of Oracle CX Sales.</td>
</tr>
<tr>
<td>Oracle Applications Cloud Configuring Applications Using Application Composer</td>
<td>Describes how administrators and implementors can make application changes using the available configuration toolset.</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oracle Applications Cloud Configuring and Extending Applications</td>
<td>Describes how to use runtime tools such as Page Composer or flexfields to configure and extend Oracle Applications Cloud.</td>
</tr>
<tr>
<td>Oracle CX Understanding Import and Export Management for CX Sales and B2B Service</td>
<td>Describes how to import and export business data into and from the CX Sales and B2B Service offerings.</td>
</tr>
<tr>
<td>Oracle CX Security Reference for CX Sales and B2B Service</td>
<td>Provides a reference to roles, role hierarchies, privileges, and policies as delivered for the Oracle CX Sales and B2B Service offerings.</td>
</tr>
<tr>
<td>Oracle CX Sales Creating and Administering Analytics</td>
<td>Explains how to view and work with analytics and reports.</td>
</tr>
<tr>
<td>Oracle CX Sales and B2B Service Subject Areas for Transactional Business Intelligence</td>
<td>Provides information about the Oracle Business Intelligence subject areas and the job roles and duty roles that secure access to each subject area.</td>
</tr>
<tr>
<td>Oracle CX Implementing Customer Data Management for CX Sales and B2B Service</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>
<tr>
<td>Oracle CX Sales Security Reference for Incentive Compensation</td>
<td>Provides a reference of roles, role hierarchies, privileges, and policies as delivered for Incentive Compensation.</td>
</tr>
<tr>
<td>Oracle CX Sales Implementing Incentive Compensation</td>
<td>Describes how to configure and set up Incentive Compensation.</td>
</tr>
</tbody>
</table>

Related Topics

- Oracle Help Center
2 Authentication

Authentication and Identity Management

Read this topic for a quick overview of 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 in 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. But 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

You can opt to use single sign-on as your user authentication solution. Single sign-on enables users to sign in to a system using one set of credentials to access multiple applications.

You can set up Oracle Applications Cloud to operate as your single sign-on service provider. Doing so provides users with single sign-on access to applications and systems located across your enterprise network. Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they’re automatically signed out from all applications on the network. For information on configuring single sign-on, see the chapter Single Sign-On.
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 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. This diagram shows the relationship between users, roles, and privileges.

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

- Job roles, which provide users with the permissions they need to perform tasks that are specific to a job, such as a sales representative
- Abstract roles, which provide users with the permissions to complete tasks that are common to all users

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 this access:

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

When the user signs in to the application and is successfully authenticated, a user session is established 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

- Role Provisioning
Predefined Sales and Service Roles

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

Sales Roles

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

If you’re using the incentive compensation functionality, you can also assign the following abstract roles to users:

• Incentive Compensation Participant
• Incentive Compensation Participant Manager

Service Roles
A number of job roles and duty roles are predefined in the Service offering. These are the predefined job roles specific to this product area:

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

Roles for Workflow Administration Access
Predefined roles provide access to workflow administration functionality. Users with the workflow roles can perform tasks such as setting up approval rules and managing submitted approval tasks. This table 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</td>
</tr>
<tr>
<td></td>
<td>BPMWorkflowCRMAadmin</td>
<td>Customer Relationship Management Application Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Analyst</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Operations Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing VP</td>
</tr>
</tbody>
</table>
Role Types

The different types of roles provided with your sales application work together to provide users with permissions to application resources. These 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 carry out tasks 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 user’s functions in the enterprise that are independent of the job they do. These are examples of the abstract roles used in the sales application:

- Employee
- Resource

Abstract roles let users to perform tasks that are common to all employees and resources. 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 because 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 lets managers work with 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.

Role Hierarchies and Role Inheritance

Each role is a hierarchy of other roles that are linked to each other in a parent-child relationship. As this hierarchy chart shows, users are assigned job and abstract roles, which inherit duty roles and their associated privileges. Duty roles in turn can inherit privileges from subordinate duty roles. You can explore the complete structure of a job or abstract role on the Security Console.

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

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

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

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

If you want to configure the predefined security model by creating your own duty roles, then it's important to understand how duty roles are constructed. A typical duty role consists of two components: data security policies, and function security privileges. Duty roles can also inherit other duty roles.

Function Security Policies

Function security policies permit a user who's 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 can view and click the Delete button. Removing that policy removes the button from view. A function security policy is composed of:

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

Some user interfaces aren't subject to data security so some function security privileges don't have an 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 the data security policy is granted to. The role can be a duty role, a job role or an abstract role. For example, the Opportunity Sales Manager duty role.
- The business object that's being accessed, for example, opportunity. The data security policy identifies the object by its table name, for example, MOO_OPTY for opportunity.
- A data privilege that defines the actions permitted 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're in the management chain or are members of the sales team for the opportunity.

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

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

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.
Guidelines for Configuring Security

If the predefined security reference implementation doesn't fully represent your enterprise, then you can make changes. For example, the predefined Sales Representative job role includes sales forecasting privileges. If sales managers do sales forecasting in your organization, not the 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 an existing role. You can perform both tasks on the Security Console.

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

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

The typical implementation doesn't use custom duty roles.

Options for Reviewing Predefined Roles
There are a number of 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**
The following manuals describe the security reference implementation for Oracle CX Sales and B2B Service 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 Security Reference for Incentive Compensation includes descriptions of all predefined security data for Incentive Compensation.

These 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 https://docs.oracle.com/.

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

**Oracle Cloud Applications Security Console**
The Security Console is an easy-to-use administrative work area where you perform most security-management tasks.

**Security Console Tasks**
You can do these tasks on the Security Console:

- Review role hierarchies and role analytics.
- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.
Note: You use the Manage Users work area, not the Security Console, to create users and to provision users with roles.

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

Note: Oracle CX Sales and B2B Service don't use certificate functionality.

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

Security Console Access
You must have the IT Security Manager job role to use the Security Console. You open the Security Console by clicking the Security Console link 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

Review the information in this chapter to learn how users gain visibility to various objects used in the sales and service applications.

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 Sales Users Gain Access to Opportunities

The security reference implementation provided by Oracle determines who can access 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’re on the opportunity sales team.
- The opportunity owner or sales team member is your direct or indirect report in the resource hierarchy.
- You’re the owner or are a member of the territory assigned to the opportunity.
- You’re the owner or member of a parent territory of the territory assigned to the opportunity.
- You’re assigned to a territory for the account associated with the opportunity.
- You’re assigned to a territory that’s a parent of the territory for the account associated with the opportunity.

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

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

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

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

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

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

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

## Special Access

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

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

- **Deal Protection:** Salespeople assigned to an opportunity retain the sales credit on an opportunity even if they're moved to another opportunity.

## How Users Gain Access to Leads

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’re the lead owner.
- The lead owner is your direct or indirect report in the resource hierarchy.
- You’re a member of the lead sales team.

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

- You’re the owner of the territory the lead is assigned to or of ancestor territories.
- You’re a member of the sales territories assigned to the lead.

## Multiple Business Units and Data Access for Sales Objects

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

A business unit (BU) is a 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 but you can create additional business units if you need to.
Users are associated with a business unit through their resource organization membership. Resource organizations are mapped to one or more business units. When you create a sales user and assign the user to a resource organization, the user gains access to each business unit that’s 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. But 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 isn't specified for a resource organization, the default business unit is used.

Within the sales application, these 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. Users also have access to transactional data for objects such as opportunities, contracts or leads:

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

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

<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>- You’re the owner or member of the territory that's assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>- You’re the owner or member of an ancestor territory of the territory assigned to the object.</td>
</tr>
<tr>
<td></td>
<td>- 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>- 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>- You're a member of the sales 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 in these ways:

- 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. So 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.

But business unit assignment can 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's assigned to the user's territory team.

For additional information about using multiple business units, see the Oracle CX Sales Implementing Sales guide.

Related Topics
- Oracle CX Sales Implementing Sales
- Overview of Sales Resources and Multiple Business Units
- Associate Resource Organizations with Multiple Business Units

Data Sharing and Visibility in Incentive Compensation

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

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

- Business unit
- Analyst assignment
- Person security profile
Business Unit

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

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

Analyst Assignment

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

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

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

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

Person Security Profile

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

Data Sharing and Visibility in Service

A service application user’s access to service requests is determined by the set of data security policies assigned to all the roles the user is provisioned with. The predefined roles in the service application don’t provide for service request visibility based on business unit or queue. But you can configure either queue or BU-based visibility to service requests for specific roles. Users assigned these roles can see only the service requests assigned to the business unit or queue where they’re a resource member.

For more information about restricting service request visibility by business unit or by queue, see the Implementing B2B Service guide.

Related Topics

- How You Set Up Service Request Visibility Based on Queue
• How You Set Up Service Request Visibility Based on BU
5 Set Up Applications Security

Overview of Applications Security Setup Tasks

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

- Manage Applications Security Preferences
  This task opens the Administration tab of the Security Console. Select the appropriate tab of the Security Console to set enterprise-wide preferences that affect users, roles, and notifications to application users.
- Import Users and Roles into Application Security
  This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables.
- Import User Login History
  This task runs a process that imports the history of user access to Oracle Fusion Applications.
- 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.

Import Users and Roles into Applications Security

To implement security, you use the Security Console. But 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 described here.

Run the Import User and Role Application Security Data Process

Sign in as a setup user and follow these steps:

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

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

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

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

- Update Existing Setup Data

Synchronize User and Role Information

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

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

Run the Retrieve Latest LDAP Changes Process

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

Related Topics

- Update Existing Setup Data

Application Security Preferences

There are a number of options on the Security Console that you can use to control the default behavior of functionality such as working with roles or certificates. Some of these options can be overridden, but it’s a good idea to set these options during implementation, before you start to create application users or configure your security environment.

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

- On the General subtab of the Security Console Administration tab, you can set these values:
  - Specify for how long certificates remain valid by default.
    - Note: The sales and service applications don't use certificate functionality.
  - Specify how often a warning appears to remind Security Console users to import latest user and role information.
• On the Roles subtab of the Security Console Administration tab, you can set these values:
  ◦ Specify default prefix and suffix values for copied roles.
  ◦ Specify a limit to the number of nodes that can appear in graphical representations of roles on the Roles tab of the Security Console.
  ◦ Specify whether hierarchies on the Roles tab appear in graphical or tabular format by default.

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

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

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

Set the Default User-Name Format

During implementation, you specify the default format of user names for users in the default user category. The default format 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.

Specify the Format of User Names

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

   The Administration page of the Security Console opens.

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

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

<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. Email is the default format.</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. Because user names generated from party or person numbers can be difficult to remember you might prefer not to 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, a user name rule will fail if the default user name format is party number or email but these values aren’t available when the user is created.
   - If the option is enabled, a system user name is generated by applying these options in the following order until a unique user name is defined:
     1. Email
     2. FirstName.LastName
     3. If only the last name is available, then a random character is prefixed to the last name.
   - If the option is disabled, then an error is raised if the user name can’t be generated in the selected format.

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

**Edit User Names**

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

**Related Topics**

- Update Existing Setup Data
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 Days Before Password Expiration option.</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This value is 10 for new installations from Update 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. If the user requests password reset by selecting Settings and Actions &gt; Set Preferences &gt; Password, then this option determines whether the last password can be reused. However, when a user's password expires, the user can reuse the</td>
<td>No</td>
</tr>
</tbody>
</table>
### Password-Policy Option

<table>
<thead>
<tr>
<th>Password-Policy Option</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>last password. This option doesn't affect password reuse after expiry.</td>
<td></td>
<td></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. 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**.

### Role Preferences

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

### Copied-Role Names

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

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

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

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

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

- Channel Account Manager Custom
- ZPM_CHANNEL_ACCOUNT_MANAGER_JOB_CUSTOM

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

**Graph Nodes and Default Views**

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

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

**Overview of User Categories**

You can categorize and segregate users based on the various functional and operational requirements. A user category provides you with an option to group a set of users such that the specified settings apply to everyone in that group. Typical scenarios in which you 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 aren’t 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's 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

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

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

You can add users to a user category in three different ways:
• Create a user category and add users to it
- Add users to an existing user category
- Specify the user category for an existing user

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

Adding Users to a New User Category

To create a user category and add users:

2. Click Edit, specify the user category details, and click Save and Close.
3. Click the Users tab and click Edit.
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.
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:

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.

User-Name and Password Notifications

Users in all user categories are notified automatically of changes to their user accounts and passwords by default. These notifications are based on notification templates. During implementation, identify the notifications that you plan to use for each user category and disable any that aren't needed. Many templates are predefined, but you can also create
templates for a user category. 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></td>
<td>Users can request new passwords by selecting the <strong>Forgot Password</strong> link on the application Sign In page, or by selecting the Password option on the Preferences page (<strong>Settings and Actions &gt; Set Preferences</strong>).</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 but you can create new templates and disable the predefined versions. Each predefined event can be associated with only one enabled notification template at a time.

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

Related Topics

- Oracle Human Capital Management Cloud Securing HCM

Create a Notification Template

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

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>
<th>Events</th>
</tr>
</thead>
</table>
| userLoginId | User name  | • Forgot user name  
<p>|           |            | • Password expired    |</p>
<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>firstName</td>
<td>User’s first name</td>
<td>• Password reset confirmation</td>
</tr>
<tr>
<td>lastName</td>
<td>User’s last name</td>
<td>All events</td>
</tr>
<tr>
<td>managerFirstName</td>
<td>Manager’s first name</td>
<td>• New account created - manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset confirmation - manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset - manager</td>
</tr>
<tr>
<td>managerLastName</td>
<td>Manager’s last name</td>
<td>• New account created - manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset confirmation - manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset - manager</td>
</tr>
<tr>
<td>loginURL</td>
<td>URL where the user can sign in</td>
<td>• Expiring external IDP signing certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password expired</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password expiry warning</td>
</tr>
<tr>
<td>resetURL</td>
<td>URL where the user can reset his or her password</td>
<td>• New account created - manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• New user created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password reset - manager</td>
</tr>
<tr>
<td>CRLFX</td>
<td>New line</td>
<td>All events</td>
</tr>
<tr>
<td>SP4</td>
<td>Four spaces</td>
<td>All events</td>
</tr>
<tr>
<td>adminActivityUrl</td>
<td>URL where an administrator initiates an administration activity</td>
<td>Administration activity requested</td>
</tr>
<tr>
<td>providerName</td>
<td>External identity provider</td>
<td>Expiring external IDP signing certificate</td>
</tr>
<tr>
<td>signingCertDN</td>
<td>Signing certificate</td>
<td>Expiring external IDP signing certificate</td>
</tr>
<tr>
<td>signingCertExpiration</td>
<td>Signing certificate expiration date</td>
<td>• Expiring external IDP signing certificate</td>
</tr>
</tbody>
</table>
### Schedule 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.

### Schedule 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.

---

<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryptionCertExpiration</td>
<td>Encryption certificate expiration date</td>
<td>Expiring service provider encryption certificate</td>
</tr>
<tr>
<td>adminFirstName</td>
<td>Administrator’s first name</td>
<td>• Administration activity location based access disabled confirmation</td>
</tr>
<tr>
<td>adminLastName</td>
<td>Administrator’s last name</td>
<td>• Administration activity single sign-on disabled confirmation</td>
</tr>
</tbody>
</table>
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.

**Review 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.

**Schedule the Import User Login History Process**

During implementation, you perform the **Import User Login History** task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables. This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform **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.

**Schedule the Process**

Follow these steps:

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

**Related Topics**

- Inactive Users Report

**Why you Run the Send Pending LDAP Requests Process**

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

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

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

- Work e-mails.
  If you include work e-mails when you create person records, then the process sends those e-mails to the LDAP directory.

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

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

  **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.

### Schedule the Send Pending LDAP Requests Process

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

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

### Schedule the Send Pending LDAP Requests Process

Follow these steps:

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

6. **Click Advanced.**
7. On the Schedule tab, set **Run** to **Using a schedule**.
8. In the **Frequency** field, select **Daily**.
9. Enter the start and end dates and times.
10. **Click Submit.**

### Give Users the Permission to View All Scheduled Processes

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

1. **Open the Security Console.**
2. **Click the Roles tab.**
3. **On the Roles tab, click Create Role.**

The Create Role page displays a series of steps you can click directly or reach using the **Next** button.

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

![Create Role Monitor ESS Processes: Basic Information](image-url)
<table>
<thead>
<tr>
<th>Field</th>
<th>Suggested Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
<td>Monitor ESS Processes</td>
</tr>
<tr>
<td>Role Code</td>
<td>MonitorESSProcesses</td>
</tr>
<tr>
<td>Role Category</td>
<td>Common -Abstract Roles</td>
</tr>
</tbody>
</table>

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

![Role Hierarchy step](image)

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

![Add Role Membership Window](image.png)

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

   The Users step should list all of the users you added.

12. Click **Next** to get to the **Summary and Impact Report** step.
13. Click **Save and Close**.

   The users you added to the role can now monitor all of the scheduled processes in the **Schedule Processes** work area.
6 Bridge for Microsoft Active Directory

Overview

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.

Caution: The bridge for Microsoft Active Directory is on limited availability only. New implementation isn't supported.

The current configuration of the bridge supports single Active Directory Forest with a single domain controller topology. The bridge uses REST API (Representational State Transfer) over HTTPS to communicate with the Oracle Applications Cloud and the LDAP (Lightweight Directory Access Protocol) to communicate with the Active Directory server. The Microsoft Active Directory server may not be reachable outside the corporate firewall but must be reachable from the computer hosting the bridge.

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.

System Requirements for the Bridge:

- RAM and CPU: As per the OS requirements
- Disk Space: Minimum 10 GB of free space

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

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
Active Directory Synchronization

The bridge for Active Directory synchronizes user account information between Oracle Applications Cloud and Microsoft Active Directory.

After you provide the bridge configuration details, install and run the bridge for Active Directory. Save the credentials to access Active Directory and Oracle Fusion Application, then return to Security Console AD Bridge setup to complete the user account mapping configuration. When mapping is complete, return to the bridge application and initiate the initial synchronization of users between the source and target applications.

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 manually 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 Forced 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 hasn't changed.
- The Run Full Synchronization button isn't clicked.

Incremental synchronization can be either on-demand (manually) or at regular intervals (automatically).
User Account Attribute Mapping

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

**Caution:** Don't use Active Directory Bridge with SSO Chooser enabled, as it will cause synchronization issues. If you sign in to Oracle Applications Cloud locally and create new users, they won't reflect in the Active Directory after synchronization.

Map the following user attributes:

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

Mapping User Attributes

The following attributes of an Oracle Fusion Applications 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 to the mapped target attributes. Some Active Directory attributes have size restrictions. For example, length of the `sAMAccountName` attribute is limited to 20 characters when used as a user attribute and can be up to 64 characters when used to name groups. Synchronization will fail if the user name has a larger value than the Active Directory attribute configured.

The following table lists a typical mapping of attributes when Oracle Fusion 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><code>emails.value</code></td>
<td>Mail</td>
</tr>
<tr>
<td>Username</td>
<td>cn</td>
</tr>
<tr>
<td><code>displayName</code></td>
<td><code>displayName</code></td>
</tr>
<tr>
<td><code>name.familyName</code></td>
<td><code>sn</code></td>
</tr>
<tr>
<td><code>name.givenName</code></td>
<td><code>givenName</code></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

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

### Microsoft Active Directory Bridge Setup

#### Prepare Oracle Applications Cloud to Connect With Microsoft Active Directory

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

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:
### Field | Description
--- | ---
Source of Truth | Select the source, such as Oracle Fusion Applications or Active Directory.
Synchronization Interval (Hours) | Enter the time interval (in hours) that the bridge uses to begin synchronization automatically. The default value is one hour.
Synchronization Paging Size | Enter the number of accounts that are synchronized in a single operation. The default value is 100 records.
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. When enabled, the synchronization will read groups the users are directly or indirectly assigned to in Active Directory. If a user has been assigned to or removed from a group of the group mapping, the corresponding user in Oracle Applications Cloud will be added to or removed from the corresponding mapped role in Oracle Applications Cloud.
Reset APPID Password | Enter a new password. During synchronization, this password is used by the bridge to connect to Oracle Applications Cloud.

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 <code>ad_fa_synch.log</code></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.
### Field Description

<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>
</tbody>
</table>
| Synchronization Strategy | Select the algorithm that must be used for synchronization. You can select **Directory Synchronization** or **Update Sequence Number**. The default value is **Directory Synchronization**.  
  **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.          |
| Search Base            | Enter the same value as the User Base DN.                                                                                                      |
| User Search Filter     | Enter the LDAP query that’s 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.                               |
  **Note:** This field is applicable only when Active Directory is the source. |
| Group Search Filter    | Enter the LDAP query that’s 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. |

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartbeat Interval</td>
<td>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.</td>
</tr>
</tbody>
</table>

9. Click **Save** and click **OK**.

**Download and Install the Bridge for Active Directory**

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 Applications Cloud and your Microsoft Active Directory server instance. Before you configure and install the bridge, ensure that you have the IT Security Manager role (ORA_FND_IT_SECURITY_MANAGER_JOB) access.

1. Click **Navigator > Tools > Security Console**.
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.
8. Click **OK**.

The bridge for Active Directory is installed. Once the bridge is installed, you can open it.
9. Click **Run** to start the bridge.
10. Enter **User name** and **Password**. You can use your Oracle Applications Cloud credentials to sign in.
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. Use the **Reset APPID Password** that you provided while configuring the bridge.
16. You can change the Oracle Applications Cloud 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.

### Map Attributes and Groups for Synchronization

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 > Tools > Security Console**.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click **User Attribute Mappings**.
4. Two attributes appear by default. Select source and target use attributes from the lists. Click **Add** to map more attributes between the source and target.
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**.

### Perform Initial Synchronization

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 Fusion 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**.
Run Synchronization

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's used to run the service. The account must have administrative and Log on as a service 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.

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).

Uninstall the Bridge for Active Directory

You can uninstall the bridge for Active Directory when you don't need it. If you had earlier installed the Windows Service associated with Active Directory Bridge, you must uninstall that service before uninstalling the Bridge for Active Directory.

Uninstall Windows Service

1. Open the bridge application and click Uninstall Windows Service on the Service Uninstall tab.
2. Review the confirmation message that appears and click OK.
3. Close the bridge application.
Uninstall the Bridge for Active Directory

1. Go to Control Panel > Programs and Features.
2. Select Bridge for Active Directory and click Uninstall.
3. Review the message that appears and click OK.
4. Enter User name and Password. Use the same credentials that you used to sign into Oracle Applications Cloud.
5. Click OK to finish the uninstallation process.
6. Delete the folder APPDATA\Oracle\AD Bridge to remove all traces of Active Directory Bridge.

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 can I synchronize information?

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 Active Directory objects can I synchronize?

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:

<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>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------</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 Location Based Access

Overview

You can use location based access to control user access to tasks and data based on their roles and computer IP addresses.

Let's take an example to understand how location based access is useful. You want your users to have complete access to tasks or features when they're signed into the application from your office network. But you want to restrict the access if the users are signing in from a home computer or an internet kiosk. To control the user access, you need to enable location based access and register the IP addresses of your office computers on the Security Console. Users have complete access to the tasks or features if they sign in from office computers. If they sign into the application from an unregistered computer, they can view and access only the generic tasks that aren't tied to any particular role. From an unregistered computer, they can't access the role-based tasks, which they could access from office.

Who Can Enable Location-Based Access

You must have the IT Security Manager role to enable location based access and make a role public. You can make a role public only when location based access is enabled. To enable location based access, you must register the IP addresses of computers from which the users usually sign in to the application.

What Happens When You Enable Location-Based Access

When you enable location based access, users signing into the application from registered IP addresses have complete access to all tasks. On the other hand, users signing in from unregistered IP addresses have no access to their role-based tasks and data. However, you can grant complete access to these users too, when required. You can also grant public access (access from all IP addresses) to certain roles. The users associated with those roles can access all tasks, no matter which IP address they sign in from.

How Location-Based Access Works

Location-based access combines the registered IP addresses of the computers and public roles to control access to the application.

Scenarios

To understand how location-based access works, consider the following scenarios and their effect on user access.

To avoid any access-related issue, carefully examine the given scenarios and plan well before you enable location-based access.
### Scenario | Impact on User Access
--- | ---
You disable location-based access. | All users signing into the application from their respective computers continue to have the same level of access as they had earlier.
You enable location-based access and register few IP addresses, but don't grant public access to any role. | • Users who sign into the application from the registered IP addresses have access to their tasks as usual.
• Users signing in from unregistered IP addresses can access only the generic tasks that aren't tied to any particular role.
You enable location-based access, register a few IP addresses, and grant public access to certain roles. | • Users signing in from the registered IP addresses have complete access.
• Users signing in from unregistered IP addresses can't access any role-based tasks unless you grant public access to those roles. If you have made a role public, users can access all the tasks tied to that role.
You enable location-based access, but don't register any valid IP address, and don't grant public access to any role. | All users are locked out. No one can sign in.

Caution: Try and avoid this scenario. Register at least one valid IP address and grant public access (access from all IP addresses) to IT Security Manager role when you enable location-based access.

### Enable and Disable Location-Based Access

You can enable location-based access so that you can allow users to access tasks and data based on their roles and registered IP addresses. By default, location-based access is disabled.

### Before You Start

Configure location-based access in a test environment and try it out before you configure it in a production environment. You must have the IT Security Manager role to enable location-based access. Additionally, you must:

- Set up a valid email address. When required, the location-based access control reset or recovery notification is sent to that email address.
- Add yourself to the user category for which the notification template ORA Administration Activity Requested Template is enabled.
- Keep the list of valid IP addresses ready.

### Enable Location-Based Access

1. Click **Navigator > Tools > Security Console**.
2. On the Administration page, click the Location Based Access tab.
3. Select **Enable Location Based Access**.
4. In the **IP Address Allowlist** text box, enter one or more IP addresses separated by commas. For example, 192.168.10.12, 192.168.10.0. To indicate a range of IP addresses, you may follow the Classless Inter-Domain Routing (CIDR) notation, such as 192.168.10.0/24.
Note: You can enter the IP address (IPv4 only) range suffix only up to 32 in the IP Address Allowlist text box. For example, 168.1.192.0/32 to 168.1.192.32/32.

Tip: Your computer’s IP address appears on the page. Add that IP address to the list so that your access to the application remains unaffected when you sign in from that computer.

5. Click Save.
6. Review the confirmation message and click OK.

After you enable location-based access, make the IT Security Manager’s role public to access Security Console even from an unregistered IP address.

Disable Location-Based Access

To disable location-based access, deselect the Enable Location Based Access check box. The existing IP addresses remain in a read-only state so that you can reuse the same information when you enable the functionality again. At that point, you can add or remove IP addresses based on your need.

FAQs for Location Based Access

What is allowlisting?

Allowlisting is the process of granting trusted entities access to data or applications. When you enable location based access and register the IP addresses of computers, you’re storing those IP addresses as trusted points of access. In other words, you’re allowlisting those IP addresses. Users signing in from those computers will be considered as trusted users and have unrestricted access to the application.

Why can't I see the Location Based Access tab on the Administration page?

To prevent any incorrect configuration, the profile option Enable Access to Location Based Access Control associated with the Location Based Access tab is perhaps disabled. As a result, the tab isn't visible. Contact your Application Implementation Consultant or Administrator to enable the profile option so that the Location Based Access tab appears on the Administration page.

How can I make a role public?

On the Security Console, identify the role that you want to make public. Except duty roles, you can make all roles public. On the Edit Role page, select the option Enable Role for Access from All IP Addresses and save the changes. All users associated with that role will have access to the role-based tasks, no matter which computer they’re using to sign into the application.

Note: You can make a role public only if location based access is enabled.
How can I ensure that I always have access to the Security Console?

If location based access is enabled, you must add your computer’s IP address to the allowlist. Also ensure that the IT Security Manager role is granted public access. Even if you have to sign in from an unregistered computer, you can still access the Security Console and other tasks associated with the IT Security Manager role.

How can I disable Location-based Access when I am not signed in to the application?

You want to disable location-based access but you’re locked out of the application and can’t sign in to the Security Console. You must request access to the Administration Activity page using the URL provided to the administrators. Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINISTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

https://<FA POD>/hcmUI/faces/AdminActivity

Click the URL and you’re directed to a secure Administrator Activity page. Select the Disable Location Based Access option and click Submit. You receive a confirmation that location-based access is disabled. Immediately, you’re redirected to the Oracle Applications Cloud login page where you can sign in using your registered user name and password, and gain access to tasks and data as earlier.

How can I disable Location-based Access when I am locked out of the application?

If you’re locked out of the application for some reason, use the following Administration Activity URL to disable location-based access:

https://<FA POD>/hcmUI/faces/AdminActivity

Only an administration user with the IT Security Manager job role can perform this unlock operation. Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Location Based Access Disabled Confirmation Template
How many IP Addresses can I enter in the IP Address Allowlist text box?

Ensure that the number of characters of the IP Address list that you enter in the IP Addresses Allowlist text box doesn't exceed 10000 characters. If you want to include more IP addresses beyond the 10000 characters limit, then you must enable the profile option ASE_EXTEND_LOCATION_BASED_ACCESS_CONTROL_IP_STORAGE.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task Manage Administrator Profile Values.
2. Search the following Profile Option Code:
   
   ASE_EXTEND_LOCATION_BASED_ACCESS_CONTROL_IP_STORAGE

3. In the Profile Value drop-down list, select Yes.
4. Click Save and Close.

If your organization has a huge network of computers, then you can import a .csv file containing the list of IP addresses. If the number of characters in the file doesn't exceed 10000 characters, the import is successful. If the number of characters exceed the limit, the import completes with a warning.

Do these steps:

1. In the Setup and Maintenance work area, select All Tasks from the Show drop-down list in the Initial Users section.
2. Click Actions for the task Manage Applications Security Preferences.
3. Click Import from CSV File, Create New.
4. Click Browse to select the file.
5. Click Submit.

If the number of characters doesn't exceed 10000, the file is imported successfully. Else, the import completes with a warning.
8 Single Sign-On

Oracle Applications Cloud as the Single Sign-On Service Provider

Your users are likely to access different internal and external applications to perform their tasks. They may require access to different applications hosted by partners, vendors, and suppliers. Certainly, users won't like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.

Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

Initial Login

On a typical working day, when users sign in for the first time, they request access to an application or a web page. Oracle Applications Cloud, which is set up as a service provider, sends a verification request to the user's identity provider who's already added to the Security Console. The identity provider verifies the user credentials and sends the authorization and authentication response back to the service provider. After successful authentication, users are granted access to the required application or web page. Because the authentication is valid across your enterprise network, users don't have to sign in again when accessing different applications available on the same network. This entire trust chain between the service provider and the various identity providers is established using the Security Assertion Markup Language (SAML) 2.0 standards.

Final Sign-out

Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they're automatically signed out from all applications on the network. This is to prevent unauthorized access and to ensure that data remains secure all the time.

Configure Single Sign-On

To enable single sign-on in your environment, complete the settings in the Single Sign-on Configuration section on the Security Console. This configuration lets you enable a login page and a page to which users must be redirected after logging out of the application. If single sign-on is enabled in your environment but you don't want it, then you can disable it using the corresponding button. By default, this button is disabled.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. In the Single Sign-On Configuration section, click **Edit**.
3. Enter the **Sign Out URL**. Users are redirected to this page once they sign out from the application.
Note: The Sign Out URL is the same for all the identity providers that you configure.

4. If Enable Chooser Login Page isn't enabled already, select it to display the service provider's single sign-on page along with your company's login page.

5. Click Save.

To configure Oracle Applications Cloud as the service provider, you must do the following:

- Add an identity provider
- Review the service provider details
- Test the identity provider
- Enable the identity provider

On the Security Console, go to the Single Sign-On tab and click Create Identity Provider.

Note: Oracle Cloud Applications support all SAML 2.0 compatible federation servers.

Add an Identity Provider

You can add as many identity providers as required to facilitate single sign-on for all your users. However, one of them must be the default identity provider.

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn't complete.

Note: Including encryption certificate in the metadata file is optional.


2. On the Identity Provider Details page, click Edit and enter the identity provider details:
   - Provide a Name and Description for the identity provider.
   - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select Email. Otherwise, leave it as Unspecified.
   - Enter the Relay State URL. Users are directed to this URL to sign and authenticate irrespective of which application they want to access.
   - Select the Default Identity Provider check box to make this identity provider the default one.

3. Import the identity provider metadata:
   - If it's an XML file, click Browse and select it.
   - If it's available on a web page, select the External URL check box and enter the URL. External URL isn't stored in this configuration and is used only for importing the identity provider metadata during identity provider creation or modification.

Note: The metadata XML file must be Base64 encoded.

4. Click Save and Close.
Review Service Provider Details

The Service Provider Details and the Diagnostics and Activation tabs are enabled only if the identity provider details are entered. Click the Service Provider Details tab and review the following information available on the page:

- ID of the service provider. In this case, it's the ID of Oracle Applications Cloud.
- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

You must share these details with the identity providers so that they can use them to configure your application as the associated service provider.

Test the Identity Provider

Click the Diagnostics and Activation tab to verify if the identity provider that you added works as expected.

1. Click the Test button to run the diagnostics. The Initiate Federation SSO page appears.
2. Click the Start SSO button. You're prompted to enter the user credentials of any user registered with the identity provider. The test validates whether the federation single sign-on is successful or not. The result summary includes the following details:
   - Status of authentication: success or failure
   - The attributes passed in the assertion
   - The assertion message in XML

You can review the log messages that appear in the Federation Logs section to identify if there are any configuration issues with the identity provider.

**Note:** You must run the test whenever there's a change in the identity provider configuration.

Enable the Identity Provider

If everything looks fine, you can go ahead and enable the identity provider. While you're on the Diagnostics and Activation page, click Edit and select the Enable Identity Provider check box. The identity provider is now active.

**Note:** You can enable an identity provider only after you import service provider metadata into the identity provider.

FAQs on Single Sign-On

Does the service provider store user passwords?

No. Passwords are stored with the identity providers. When a user signs in, the identity provider authenticates the password, authorizes the request to access an application, and sends that confirmation back to the service provider. The service provider then allows users to access the application or web page.
Can I set up an identity provider without enabling it?
Yes, you can set up an identity provider and test it thoroughly before enabling it. By default, an identity provider remains disabled. You can disable an identity provider at any time.

How can I allow my users to sign in using their company's credentials?
On the Security Console, go to Single Sign-On > Identity Provider Details page and make sure that the Enable Chooser Login Page check box is selected.
When your users access the main portal page, they can sign in using one of the following options:

- The single sign-on credentials registered with the identity provider
- The single sign-on credentials registered with their company

What should I do to extend the validity of certificates provided by the identity provider?
Pay attention to the notifications you receive about certificate expiry. Request your identity provider to share with you the updated metadata file containing renewed certificate validity details. Once you upload the metadata file, the validity of the certificate is automatically renewed. You will have to monitor this information at intervals to ensure that the certificates remain valid at all times.

How can the identity provider obtain renewed certificates from the service provider?
The identity provider can submit a service request to the service provider asking for the renewed signing and encryption certificates.

How can I disable Single Sign-On when I am not signed in to the application?
You must request access to the Administration Activity page using the URL provided to the administrators. Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINISTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:
https://<FA POD>/hcmUI/faces/AdminActivity

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Single Sign On** option and click **Submit**. You receive a confirmation that single sign-on is disabled. Immediately, you're redirected to the Oracle Applications Cloud login page where you can sign in using your registered user name and password.

How can I disable Single Sign-On when I am locked out of the application?

If you're locked out of the application for some reason, use the following Administration Activity URL to disable single sign-on:

https://<FA POD>/hcmUI/faces/AdminActivity

Only an administrator user with the IT Security Manager job role can perform this unlock operation.

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Single Sign-On Disabled Confirmation Template

What are the different events and notifications associated with the Single Sign-On functionality?

Automatic notifications are sent for the following events associated with single sign-on:

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled
- When the external identity provider's signing certificate is about to expire
- When the service provider's signing certificate is about to expire
- When the service provider’s encryption certificate is about to expire

**Note:** Notifications are sent to users who are assigned the **Manage SSO** privilege, as per the following schedule:

- First notification - 60 days before the expiry date
- Second notification - 30 days before the expiry date
- Last notification - 10 days before the expiry date.

How do I reimport Identity Provider metadata?

Whenever you get an updated metadata file from the Identity Provider you must reimport the file into the application to continue using SSO configuration

1. On the Identity Provider Details page, click **Edit**.
2. Import the identity provider metadata:
   - If it's an XML file, click **Browse** and select it.
- If it's available on a web page, select the **External URL** check box and enter the URL.

  **Note:** The metadata XML file must be Base64 encoded.

3. Click **Save and Close**.

  **Note:** Remember to test the Identity Provider after reimport.
9 API Authentication

Configure Outbound API Authentication Using JWT Custom Claims

A system account is an account used for integrating Oracle Applications Cloud with third-party applications. This account isn't associated with a user but it must have roles with access to REST APIs. System account uses basic authentication to authenticate users even if single sign-on is enabled. Security Console’s password policy applies to a system account and so the password of this account expires based on the password policy.

Critical tasks such as batch operations or data synchronizations must continue without any interruption or the need to re-authenticate at intervals. To support such tasks, you need to define custom parameters for authentication. Using Security Console, you can define a JSON Web Token (JWT) that can be used by REST APIs to automate system authentication without you having to authenticate manually.

JWT is an access token that contains custom claim name and claim values. Custom claims are name and value pairs that you can define in a JWT. To uniquely identify a user, you can add the user's email address to the token along with the standard user name and password.

Example, suppose you want to integrate Oracle Applications Cloud with a third-party application. This integration uses the JWT Custom Claims to authenticate the users who sign into Oracle Applications Cloud to access the third-party application.

Do these steps to define a JWT that will be used for integration with third-party application:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**, **Edit**.
3. Enter a name and description for the external client application that you want to create.
4. In the **Select Client Type** drop-down list, select **JWT Custom Claims** and click **Save and Close**.
5. Click the JWT Custom Claims Details tab and click **Edit**.
6. In the Token Settings section, if required, update the **Token Expiration Time** and **Signing Algorithm**. Default values are 30 minutes and RS256 respectively.
7. Click **Save**.
8. In the JWT Custom Claims section, click **Add**. You can either select a name from the predefined values in the drop-down list or select **Other** and enter a name of your choice.
9. Select a value for the custom claim. If you select **Free-form**, enter the value in the following text box. You can add more JWT custom claims using the **Add** button.
10. Click **Save**. You can add more parameters as required.
11. Click **Done** to return to the JWT Custom Claims Details page.

You can view the token created for authentication using the **View JWT** button on the JWT Custom Claims Details page. The View JWT window displays the header and payload of the JWT.

12. Click **Done** again to return to the API Authentication page. You can view the newly created JWT Custom Claim in this page.

You can delete a JWT custom claim on the API Authentication page.
Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol

OAuth is an open industry standard protocol that allows applications access information from other third-party applications, on behalf of the users. The OAuth authorization protocol manages access securely without revealing any passwords to the client application, such as Oracle Applications Cloud.

To understand the OAuth authorization protocol, let’s take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required permissions to Oracle Applications Cloud to access the information from LinkedIn.

As you notice, there are three parties involved in the entire authentication process: Oracle Applications Cloud, the user who owns information on LinkedIn, and LinkedIn's authorization server. This authorization protocol always requires three such parties for the authentication to complete. Therefore, this protocol is called three-legged OAuth authorization protocol.

Here’s the sequential representation of the end-to-end authorization process between Oracle Applications Cloud and the LinkedIn server:

1. Oracle Applications Cloud registers the Client ID and Client Secret and other settings required for authorization.
2. When an Oracle Applications Cloud user wants to access profile information, the LinkedIn login page appears, where the user authenticates using the required credentials.
3. On successful authentication, LinkedIn's authorization server sends an authorization code to Oracle Applications Cloud.
4. Oracle Applications Cloud receives the authorization code and sends an access token request to LinkedIn. LinkedIn processes the access token request and returns an access token.
5. Oracle Applications Cloud uses the access token to call LinkedIn APIs on behalf of the user to access the required information. At runtime, Oracle Web Services Manager manages the entire authorization process.

The following graphic shows the entire authorization process between Oracle Applications Cloud and the LinkedIn server:
Using the Security Console, you configure the three-legged OAuth authorization settings for Oracle Applications Cloud. Once configured, users can access their information from a third-party application, within Oracle Applications Cloud.

Here’s how you configure three-legged OAuth authorization:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**.
3. On the External Client Application Details page, click **Edit**.
4. Enter a name and description for the external client application that you want to create.
5. In the **Select Client Type** drop-down list, select **OAuth Three-Legged**.
6. Click **Save and Close** to return to the External Client Application Details page.
7. Click the OAuth Details tab.
8. On the Three-Legged OAuth Details page, click **Edit**.
9. Enter the appropriate values in the following required fields:
   - Authorization URL
   - Redirect URL
   - Access Token URL
   - Servlet Application URL
   - Client ID
   - Client Secret
   - Client Scope
10. Enter the appropriate values in the following optional fields, if required:
    - Server Scope
    - Federated Client Token
    - Include Client Credential
    - Client Credential Type
11. Click **Save and Close**.
12. Click **Done** to return to the Three-Legged OAuth Details page.
13. Click **Done** again to return to the API Authentication page. You can view the newly created three-legged OAuth configuration here.

### Configure Inbound Authentication

Third-party application users can access a service of Oracle Applications Cloud if inbound authentication is configured for them. You can use an Oracle API Authentication Provider to configure inbound authentication for such users. To configure inbound authentication, you need a public certificate and a trusted issuer which contains the tokens.

Oracle Applications Cloud supports the JSON Web Token (JWT), Security Assertion Markup Language (SAML), and Security Token Service (STS) tokens. Use the Security Console to configure the trusted issuer and public certificate details. The default trusted issuer is Oracle (www.oracle.com) and you can’t delete it.

We recommend that you use JWT for inbound authentication for a system account that’s created for a specific application. For authentication, JWT uses a combination of a public certificate and trusted issuer whereas a system account’s password expires soon based on the security policy. In addition, you must ensure that the system account’s credentials are valid.
How Inbound Authentication Works

When a third-party application user sends an authentication request to access a service of Oracle Applications Cloud, these actions occur in the background:

1. The third-party application generates a JWT that includes trusted issuer and public certificate information.
2. Oracle Web Services Manager authenticates the generated JWT by verifying whether the trusted issuer and public certificate are valid.
3. On successful authentication, the third-party application gets access to the Oracle Applications Cloud service.

Here's how you configure an Oracle API Authentication Provider for inbound authentication:

1. On the Security Console, click **API Authentication**.
2. Click **Create Oracle API Authentication Provider**.
3. On the Oracle API Authentication Provider Details page, click **Edit**.
4. On the API Authentication Configuration Details page, enter a name for the **Trusted Issuer**.
5. Select one or more token types that you want to include in the trusted issuer.
6. Click **Save and Close**.
7. On the Oracle API Authentication Provider Details page, click the Inbound API Authentication Public Certificates tab and click **Edit**. You can use the default Oracle public certificate or add a new one.
8. On the Inbound API Authentication Public Certificates page, click **Add New Certificate** to add a different public certificate.
9. Enter the **Certificate Alias** name.
10. Click **Browse** and select the public certificate that you want to import.
11. Click **Save**. The newly added certificate alias is displayed on the Inbound API Authentication Public Certificates page.
12. Click **Done** to return to the API Authentication page.

**Related Topics**

- Configure JWT Authentication Provider
- Reset Password for an Existing User
- Use JSON Web Token for Authorization

Is there a recommended format for the public certificate?

Yes. Oracle recommends that the public certificate you upload must contain only line feed (denoted by the code `\n`) to indicate separation of lines. Because carriage return isn't supported, make sure that the certificate doesn't contain carriage return along with the line feeds.
10 Export and Import of Security Setup Data

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV export and import functionality.

Let’s assume you have spent a lot of time and effort in configuring and setting up the Security Console in your primary environment. You test the setup and find that everything’s working as intended. Now, you want to replicate the same setup in another environment. And you want that to happen with the least effort and as quickly as possible. Well, it certainly can be done in a simple and less time-consuming way.

In the Setup and Maintenance work area, use the Manage Application Security Preferences task in the Initial Users functional area.

Before You Begin

Learn how to export business object data to a CSV file and to import business data from a CSV file. Detailed instructions are available in the Managing Setup Using CSV File Packages chapter of the Using Functional Setup Manager guide.

What Gets Exported and Imported

The Security Console setup data comprises information that you see on the Administration and User Categories tabs of the Security Console. The following business objects help in packaging those details into CSV files so that the data can be easily exported and imported.

- Security Console Administration Settings
- Security Console User Category
- Security Console User Category Notifications

| Note: Lists of users or information about any specific user is never a part of this export and import process.

In this table, you will find information about the contents of each business object.

<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Console Administration Settings</td>
<td>• General administration details</td>
</tr>
<tr>
<td></td>
<td>• Role preferences</td>
</tr>
<tr>
<td></td>
<td>• Location-based access settings</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If location-based access isn’t enabled (if the tab doesn’t appear on Security Console), nothing gets included in the export or import.</td>
</tr>
<tr>
<td>Security Console User Category</td>
<td>• User category details</td>
</tr>
<tr>
<td></td>
<td>• Password policy information</td>
</tr>
</tbody>
</table>
Export and Import of Security Setup Data

### Business Object

<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Console User Category Notifications</td>
<td>Notification preferences.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For notifications, only the custom template information is exported from the default user category. The predefined notifications are excluded because they're available in the target environment.</td>
</tr>
</tbody>
</table>

When the export process successfully completes, you get the following CSV files:

- Administration Settings CSV
- User Category CSV
- User Category Notifications CSV

**Note:** If there are language packs installed on your application, additional CSV files may be generated containing the translated data.

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

**Related Topics**

- Export and Import CSV File Packages
- Key Information About Setup Data Export and Import Processes

### Export and Import of HCM Custom Roles and Security Profiles

You're looking at migrating your HCM custom roles, data roles and security profiles from one environment to another. You can accomplish most of your HCM security migration needs by exporting the business objects in the Users and Security functional area within the Workforce Deployment offering. The exception to this is Job Requisition Security profiles, which can be migrated by exporting the business objects in the Users and Security functional area within the Recruiting and Candidate Experience offering.

Other offerings have a Users and Security functional area, but only the Workforce Deployment offering has the business objects that support migration of HCM custom roles within its Users and Security functional area.

### Before You Begin

Learn how to export and import business object data. Detailed instructions are available in the Overview of Setup Data Export and Import topic of the Using Functional Setup Manager guide. Refer to the Related Topics section for the link to this topic.
What Gets Exported and Imported

When you migrate HCM roles and security profiles, the following business objects are exported in the configuration package at generated from the Users and Security functional area within the Workforce Deployment offering.

- Application Data Security
- Application Profile Value
- Functional Security Custom Roles
  - Functional Security Custom Role Hierarchy
  - Functional Security Custom Role Privilege Membership
- HCM Data Role
  - HCM Data Role Security Profile
- HCM Exclusion Role
  - HCM Exclusion Rule Detail
- Legislative Data Group Security Profile
  - Legislative Data Group Security Profile List
- Organization Security Profile
  - Organization Security Profile Classification List
  - Organization Security Profile Organization List
- Country Security Profile
  - Country Security Profile Country List
- Position Security Profile
  - Position Security Profile Position List
  - Position Security Profile Area of Responsibility Scope
- HR Document Type Security Profile List
  - HR Document Type Security Profile List
- Payroll Security Profile
  - Payroll Security Profile Pay
- Payroll Flow Security Profile
  - Payroll Flow Security Profile Pay
- Person Security Profile
  - Person Security Profile Manager Type
  - Person Security Profile Area of Responsibility Scope
  - Person Security Profile Exclusion
Let's closely examine each business object to know what it contains.

<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Data Security</td>
<td>Application data security includes data security policies that are created in the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Manually using the Manage Database Resources page in the security console.</td>
</tr>
<tr>
<td></td>
<td>• Manually using the Edit role/Copy role flow in the security console</td>
</tr>
<tr>
<td></td>
<td>• Automatically when you copy a role using the Role Copy in the security profile</td>
</tr>
<tr>
<td></td>
<td>• Automatically when you create profile content types</td>
</tr>
<tr>
<td></td>
<td>• Automatically when you map HCM spreadsheet business objects to roles</td>
</tr>
<tr>
<td></td>
<td>Data security policies that are generated by the HCM Data Roles UI aren't exported as part of the application data security business object. They are automatically created on the target environment when you import the HCM Data Role business object.</td>
</tr>
<tr>
<td></td>
<td>Data security conditions that are generated from HCM security profiles aren't exported as part of the Application Data security business object. They are automatically created on the target environment when the HCM security profile business objects are imported.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> there's no scope support for application data security policies. When you export application data security policies all data security policies are exported, even if you provided a scope value for other security business objects in your configuration package. there's no Export to CSV option for this business object.</td>
</tr>
<tr>
<td>Application Profile Value</td>
<td>Application profile value includes the profile values for the PER_MASTER_WORK_EMAIL profile.</td>
</tr>
<tr>
<td></td>
<td>This profile option is no longer used and no values are exported for this business object.</td>
</tr>
<tr>
<td>Functional Security Custom Roles</td>
<td>The custom role includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Role Code</td>
</tr>
<tr>
<td></td>
<td>• Role Name</td>
</tr>
<tr>
<td></td>
<td>• Role Description</td>
</tr>
<tr>
<td></td>
<td>• Role Category</td>
</tr>
<tr>
<td></td>
<td>• All IP Address Access - indicates that a role is granted access to the Security Control irrespective of the IP address from where it's signed in.</td>
</tr>
<tr>
<td>Business Object</td>
<td>Information Included in Export and Import</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional Security Custom Role Hierarchy</td>
<td>The role hierarchy includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Parent Role</td>
</tr>
<tr>
<td></td>
<td>• Member Role</td>
</tr>
<tr>
<td></td>
<td>• Add or Remove Role Membership</td>
</tr>
<tr>
<td>Functional Security Custom Role Privilege Membership</td>
<td>The role privilege membership includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Parent Role</td>
</tr>
<tr>
<td></td>
<td>• Member Privilege</td>
</tr>
<tr>
<td></td>
<td>• Add or Remove Privilege Membership</td>
</tr>
<tr>
<td>HCM Data Role</td>
<td>The HCM data role includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Data Role Code</td>
</tr>
<tr>
<td></td>
<td>• Data Role Name</td>
</tr>
<tr>
<td></td>
<td>• Data Role Description</td>
</tr>
<tr>
<td></td>
<td>• Inherited Job Role Code</td>
</tr>
<tr>
<td></td>
<td>• Delegation Allowed Check Box</td>
</tr>
<tr>
<td>HCM Data Role Security Profile</td>
<td>The HCM data role security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Data Role Code</td>
</tr>
<tr>
<td></td>
<td>• Securing Object</td>
</tr>
<tr>
<td></td>
<td>• Security Profile Name</td>
</tr>
<tr>
<td>HCM Exclusion Rule</td>
<td>HCM exclusion rule and HCM exclusion rule detail includes HCM exclusion rule definitions.</td>
</tr>
<tr>
<td></td>
<td>• HCM Exclusion Rule</td>
</tr>
<tr>
<td></td>
<td>• HCM Exclusion Rule Detail</td>
</tr>
<tr>
<td>Legislative Data Group Security Profile List</td>
<td>Legislative data group security profile list includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Legislative data group security profile name</td>
</tr>
<tr>
<td></td>
<td>• Legislative data groups that are included in the legislative data group security profile</td>
</tr>
<tr>
<td>Organization Security Profile</td>
<td>Organization security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Organization Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td></td>
<td>• View All Check Box</td>
</tr>
<tr>
<td></td>
<td>• Include Future Organizations Check Box</td>
</tr>
<tr>
<td></td>
<td>• Code indicating Department Hierarchy or Generic Organization Hierarchy</td>
</tr>
<tr>
<td></td>
<td>• Hierarchy Name (if securing by organization hierarchy)</td>
</tr>
<tr>
<td></td>
<td>• Top Organization Name (if securing by organization hierarchy)</td>
</tr>
<tr>
<td></td>
<td>• Include Top Organization Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Organization Hierarchy Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Organization Classification Check Box</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Secure by Organization List Check Box</td>
</tr>
<tr>
<td>Organization Security Profile Classification List</td>
<td>Organization security profile classification list includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Organization Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Organization Classification Name</td>
</tr>
<tr>
<td>Organization Security Profile Organization List</td>
<td>Organization security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Organization Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Organization name</td>
</tr>
<tr>
<td></td>
<td>• Organization Classification</td>
</tr>
<tr>
<td></td>
<td>• Include/Exclude Check Box</td>
</tr>
<tr>
<td>Country Security Profile</td>
<td>Country security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Country Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td>Country Security Profile List</td>
<td>Country security profile list includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Country Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Country code</td>
</tr>
<tr>
<td>Position Security Profile</td>
<td>Position security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Position Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td></td>
<td>• View All Check Box</td>
</tr>
<tr>
<td></td>
<td>• Include Future Positions Check Box</td>
</tr>
<tr>
<td></td>
<td>• Hierarchy Name (if securing by position hierarchy)</td>
</tr>
<tr>
<td></td>
<td>• Top Position Name (if securing by position hierarchy)</td>
</tr>
<tr>
<td></td>
<td>• Include Top Position Check Box</td>
</tr>
<tr>
<td></td>
<td>• Top Position Name (if securing by organization hierarchy)</td>
</tr>
<tr>
<td></td>
<td>• Secure by Position Hierarchy Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Department Check Box</td>
</tr>
<tr>
<td></td>
<td>• Department Organization Security Profile Name (if securing by department)</td>
</tr>
<tr>
<td></td>
<td>• Secure by Business Unit Check Box</td>
</tr>
<tr>
<td></td>
<td>• Business Unit Organization Security Profile Name (if securing by business unit)</td>
</tr>
<tr>
<td></td>
<td>• Secure by Position List Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Area of Responsibility Check Box</td>
</tr>
<tr>
<td>Position Security Profile Position List</td>
<td>Position security profile position list includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Position Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Position Code</td>
</tr>
<tr>
<td></td>
<td>• Include/Exclude Check Box</td>
</tr>
<tr>
<td>Business Object</td>
<td>Information Included in Export and Import</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Position Security Profile Area of Responsibility</td>
<td>Position security profile area of responsibility scope includes the following details:</td>
</tr>
<tr>
<td>Scope</td>
<td>• Position Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Responsibility Type</td>
</tr>
<tr>
<td></td>
<td>• Scope of Responsibility</td>
</tr>
<tr>
<td>HR Document Type Security Profile</td>
<td>HR document type security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• HR Document Type Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td></td>
<td>• View All Check Box</td>
</tr>
<tr>
<td></td>
<td>• Include/Exclude Check Box</td>
</tr>
<tr>
<td>HR Document Type Security Profile List</td>
<td>HR document security profile list includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• HR Document Type Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Document Type Name</td>
</tr>
<tr>
<td>Payroll Security Profile</td>
<td>Payroll security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Payroll Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td></td>
<td>• View All Check Box</td>
</tr>
<tr>
<td>Payroll Security Profile Pay</td>
<td>Payroll security profile pay includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Payroll Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Payroll Name</td>
</tr>
<tr>
<td></td>
<td>• Legislative Data Group Name</td>
</tr>
<tr>
<td>Person Security Profile</td>
<td>Person security profile includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Person Security Profile Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td></td>
<td>• Access to Own Record Check Box</td>
</tr>
<tr>
<td></td>
<td>• Include Future People Check Box</td>
</tr>
<tr>
<td></td>
<td>• Include Shared People Information Check Box</td>
</tr>
<tr>
<td></td>
<td>• Access to Candidates with Offers Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Area of Responsibility</td>
</tr>
<tr>
<td></td>
<td>• Secure by Manager Hierarchy Check Box</td>
</tr>
<tr>
<td></td>
<td>• Person or Assignment Check Box</td>
</tr>
<tr>
<td></td>
<td>• Maximum Levels in Hierarchy</td>
</tr>
<tr>
<td></td>
<td>• Manager Hierarchy Type</td>
</tr>
<tr>
<td></td>
<td>• Hierarchy Content Code</td>
</tr>
<tr>
<td></td>
<td>• Secure by Person Type Check Box</td>
</tr>
<tr>
<td></td>
<td>• Secure by Department Check Box</td>
</tr>
<tr>
<td></td>
<td>• Department Security Profile Name (if securing by department)</td>
</tr>
<tr>
<td></td>
<td>• Secure by Business Unit Check Box</td>
</tr>
<tr>
<td></td>
<td>• Business Unit Profile Name (if securing by business unit)</td>
</tr>
<tr>
<td>Business Object</td>
<td>Information Included in Export and Import</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Secure by Legal Employer Check Box&lt;br&gt;• Legal Employer Security Profile Name (if securing by legal employer)&lt;br&gt;• Secure by Position Check Box&lt;br&gt;• Position Security Profile Name (if securing by position)&lt;br&gt;• Secure by Legislative Data Group Check Box&lt;br&gt;• Legislative Data Group Security Profile Name (if securing by legislative group)&lt;br&gt;• Secure by Payroll Check Box&lt;br&gt;• Payroll Security Profile Name (if securing by payroll)&lt;br&gt;• Secure by Global Name Range Check Box&lt;br&gt;• Global Name Range Start Value (if securing by global name range)&lt;br&gt;• Global Name Range End Value (if securing by global name range)&lt;br&gt;• Apply Exclusion Rules Check Box&lt;br&gt;• Secure by Custom Criteria Check Box&lt;br&gt;• Custom Restriction Text (if securing by custom criteria)&lt;br&gt;•</td>
</tr>
<tr>
<td>Person Security Profile Manager Type</td>
<td>Person security profile manager type includes the following details:&lt;br&gt;• Person Security Profile Name&lt;br&gt;• Manager Hierarchy Type (if something other than All or Line Manager has been selected on the security profile)&lt;br&gt;•</td>
</tr>
<tr>
<td>Person Security Profile Area of&lt;br&gt;Responsibility Scope</td>
<td>Person security profile area of responsibility scope includes the following details:&lt;br&gt;• Person Security Profile Name&lt;br&gt;• Responsibility Type&lt;br&gt;• Scope of Responsibility&lt;br&gt;• Employee Check Box&lt;br&gt;• Contingent Worker Check Box&lt;br&gt;• Pending Worker Check Box&lt;br&gt;• Nonworker Check Box&lt;br&gt;• Candidate with Offer Check Box&lt;br&gt;•</td>
</tr>
<tr>
<td>Person Security Profile Exclusion</td>
<td>Person security profile exclusion includes the following details:&lt;br&gt;• Person Security Profile Name&lt;br&gt;• Exclusion Rule Name&lt;br&gt;•</td>
</tr>
<tr>
<td>Transaction Security Profile</td>
<td>Transaction security profile includes the following details:&lt;br&gt;• Transaction Security Profile Name&lt;br&gt;• Description&lt;br&gt;• Enabled Check Box&lt;br&gt;• View All Check Box&lt;br&gt;•</td>
</tr>
<tr>
<td>Transaction Security Profile Entries</td>
<td>Transaction security profile entries includes the following details:&lt;br&gt;• Transaction Security Profile Name&lt;br&gt;• Product Family&lt;br&gt;• Category Code&lt;br&gt;•</td>
</tr>
<tr>
<td>Business Object</td>
<td>Information Included in Export and Import</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                                             | • All Sub-Categories Check Box  
|                                             | • Exclude Sub-Category Check Box  
| Transaction Security Profile Sub-Categories | Transaction security profile sub-categories includes the following details:  
|                                             | • Transaction Security Profile Name  
|                                             | • Product Family  
|                                             | • Category Code  
|                                             | • Sub-Category Code  
| Role Provisioning Rule                      | Role provisioning rule includes the following details:  
|                                             | • Mapping Rule Name  
|                                             | • Legal Employer Name  
|                                             | • Business Unit Name  
|                                             | • Department Name  
|                                             | • Job Set Code  
|                                             | • Job Code  
|                                             | • Position Business Unit Name  
|                                             | • Position Code  
|                                             | • Grade Set Code  
|                                             | • Grade Code  
|                                             | • Location Set Code  
|                                             | • Location Code  
|                                             | • User Person Type  
|                                             | • System Person Type  
|                                             | • Assignment Type  
|                                             | • HR Assignment Status Code  
|                                             | • Resource Role  
|                                             | • Party Type Usage Code  
|                                             | • Contact Role  
|                                             | • Manager with Reports Check Box  
|                                             | • Manager Type  
|                                             | • Responsibility Type  
| Role Provisioning Associated Role List      | Role provisioning associated role list includes the following details:  
|                                             | • Mapping Rule Name  
|                                             | • Role Code  
|                                             | • Requestable Check Box  
|                                             | • Self-Requestable Check Box  
|                                             | • Autoprovision Check Box  

Other business objects that you might like to export when migrating HCM custom roles are:

- Job Requisition Security Profile
- Spreadsheet Business Object Security Mapping

Let's closely examine each of these business objects to know what they contain.
### Business Object

<table>
<thead>
<tr>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Requisition Security Profile</td>
</tr>
<tr>
<td>Job requisition security profile includes the following details:</td>
</tr>
<tr>
<td>• Job Requisition Security Profile Name</td>
</tr>
<tr>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td>• View All Check Box</td>
</tr>
<tr>
<td>• Secure by Job Family Check Box</td>
</tr>
<tr>
<td>• Secure by Job Function Check Box</td>
</tr>
<tr>
<td>• Secure by Location Check Box</td>
</tr>
<tr>
<td>• Secure by Organization Check Box</td>
</tr>
<tr>
<td>• Secure by Recruiting Type Check Box</td>
</tr>
<tr>
<td>Spreadsheet Business Object Security</td>
</tr>
<tr>
<td>Mapping</td>
</tr>
<tr>
<td>HCM spreadsheet business object access mapping includes the following details:</td>
</tr>
<tr>
<td>• Role Code</td>
</tr>
<tr>
<td>• Business Object</td>
</tr>
<tr>
<td>• Product Area</td>
</tr>
<tr>
<td>• Enabled Check Box</td>
</tr>
<tr>
<td>• All Business Objects Check Box</td>
</tr>
</tbody>
</table>

You can migrate job requisition security profiles by exporting the business objects in the Users and Security functional area within the Recruiting and Candidate Experience offering. You should do this prior to migrating the business objects in the Users and Security functional area within the Workforce Deployment offering. You must have the Recruiting Administrator role to export and import job requisition security profiles.

You can migrate HCM spreadsheet business object access mappings by exporting the business objects in the HCM Data Loader functional area within the Workforce Deployment offering. You should do this after migrating the business objects in the Users and Security functional area. You must have the Human Capital Management Integration Specialist role to export and import HCM spreadsheet business object access mappings.

### After the Import Completes

You may need to wait for a period of time before all of the migrated data security policies are visible in the security console after completing the import of the configuration package that's generated from the Users and Security functional area within the Workforce Deployment.

When application data security policies are imported, a process runs in the background to synchronize the imported data security policies with the roles on the target environment. The imported data security policies aren't active until this process has completed, at which point the data security policies will be visible in the security console. This affects data security policies for custom roles that have been copied from other roles in the source environment. It also affects custom roles that have data security policies that were added manually using the security console.

**Note:** No manual regeneration processes are needed on the target environment; the import process triggers the role regeneration process. This only applies if you're importing the HCM Data Role business object.

### What's Not Included

Data security policies that have been manually created from the security console, and which reference conditions that have been generated from an HCM security profile, must be manually recreated on the target environment. You must
import the condition by importing the appropriate HCM security profile business object before creating these data security policies in the target environment.

Related Topics

- Overview of Setup Data Export and Import
11 Sales Users and Role Provisioning

Types of Sales 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’s also a setup user if you want.

Initial Users

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

These are the roles assigned to the initial user:

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

The initial user can create each of the 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 the setup tasks. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges.

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

- Sales Analyst job role
  Makes it possible to create Sales Predictor rules.
- Sales Administrator job role
  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
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're assigned. You must create at least one sales administrator user.

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

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

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

To create sales administrators, follow the procedure outlined in the topic 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're assigned. The provisioned job roles don't permit sales users to perform implementation tasks, but they can perform a functional setup within the application, depending on their role. Provision sales application users with these roles:

- The job roles that they require to perform their job
- The Resource abstract role
- The Employee or the Contingent Worker abstract role, depending on the employee type of the user

Sales Restricted Users

To do their jobs effectively, users must be able to view all the data that's relevant to their role. In some cases, however, users don't require the ability to create, update, or delete that data. You can create sales application users who have extensive privileges to view sales data, but limited privileges to change data, by provisioning users with these roles:

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

Users assigned the Sales Restricted User job role can:

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

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

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

The Essential User license provides a user with a read-only subscription to Oracle CX Sales and B2B Service. You must provision the Sales Restricted User job role to users who are assigned an Essential User license.

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

**Related Topics**
- Create Sales Restricted Users
- Create Application Users
- Create Setup Users
- Give Users the Permission to View All Scheduled Processes
- Provide Read-Only Access for Individual Users

**Methods of Creating Sales Users**

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

• Create users individually in the Manage Users work area.
  You can navigate to this work area using the Navigator menu from any application page.
  Use this method to create setup users, and to create individual sales application users.

• Import users using the Import Management functionality or using the Quick Import Excel macros which you can download from My Oracle Support.
  Import users 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 source attributes to the attributes required by the application. You can't import setup users because the import process requires you to import sales resources. For additional information about importing users, see the following information at http://docs.oracle.com/:
  o The chapter about importing users in the guide Getting Started with Your Sales Implementation
The chapter about importing employee resources in the guide Oracle CX Understanding Import and Export Management for CX Sales and B2B Service

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

Related Topics
- Create Application Users

## 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’re 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.

**Note:** These tasks don’t apply to setup users because they’re 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>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>

**Resource Reporting Hierarchy**

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

The resource reporting hierarchy doesn't have to mirror the formal reporting hierarchy, which is captured separately in the Oracle HCM Cloud application if it has been implemented. In Oracle CX Sales and B2B Service, you can have only one resource reporting hierarchy reporting to one person.

**Resource Organizations and the Resource Organization Hierarchy**

You must assign each manager that you create as a user with his or her own resource organization. All direct reports who are individual contributors inherit their manager's organization. The application automatically builds a resource organization hierarchy, using the resource reporting structure. The resource organizations remain even if managers leave. You can reassign the resource organizations to their replacements.

In CX Sales and B2B Service, resource organizations serve a limited purpose. The name of each resource organization appears in the application's Resource Directory, which users can access to obtain information about their coworkers, and in social media interactions. However, resource organizations aren't used in application security or for work assignments. You assign work to individuals rather than their organizations.

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

**Related Topics**

- Create Application Users
Role Provisioning

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're 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 doesn’t matter if you create users manually in the user interface, or import them from a file or using the Sales User Quick Import Excel macro.

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.

Sales Resource Roles Provided by Oracle
Oracle provides you with the following standard sales organization resource roles and the appropriate job roles for each:

- Channel Account Manager
- Channel Operations Manager
- Channel Sales Manager
- Chief Executive Officer
- Contract Administrator
- Contract Manager
- Customer Data Steward
- Data Steward Manager
- Inside Sales Representative
- Inside Sales Manager
- Partner Administrator
- Partner Sales Manager
- Partner Salesperson
- Sales Administrator
• Sales Lead Qualifier
• Sales Manager
• Salesperson
• Sales Restricted User
• Sales Setup User
• Sales Vice President

Sales Role-Provisioning Rules Provided by Oracle
Oracle provides role provisioning rules for provisioning most of the standard sales job roles to users. Oracle also provides rules to assign the Employee abstract role to all active users who are created as employees, and the Contingent Worker abstract role to active non-employee users who are created as contingent workers.

The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. You perform this step after enabling your Sales or Service offering. If you set up the company information in a different way, perhaps because you’re implementing a number of cloud services at the same time, then you must create the provisioning rules yourself using the steps outlined in the topic Create Rules to Automatically Provision Job Roles to Sales Users. For information about setting up your company information, see the Getting Started with Your Sales Implementation guide.

The following table lists the role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles the rule provisions. 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.
  The HR Assignment Status condition isn't applicable to partner users who are created as external sales users. As a result, the partner provisioning rules specify only one condition, Resource Role.

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

<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>
</tbody>
</table>

The Requestable, Self-Requestable, and Autoprovision options are enabled for each role assigned by the provisioning rules.
<table>
<thead>
<tr>
<th>Provisioning Rule Name</th>
<th>Condition</th>
<th>Job or Abstract Roles Provisioned</th>
</tr>
</thead>
<tbody>
<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>Inside Sales Representative</td>
<td>HR Assignment Status is Active</td>
<td>Inside Sales Representative</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Inside Sales Representative</td>
<td>Resource</td>
</tr>
<tr>
<td>Inside Sales Manager</td>
<td>HR Assignment Status is Active</td>
<td>Inside Sales Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Inside Sales 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>
<tr>
<td>Provisioning Rule Name</td>
<td>Condition</td>
<td>Job or Abstract Roles Provisioned</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Sales Manager</td>
<td>HR Assignment Status is Active</td>
<td>Sales Manager</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Sales Manager</td>
<td></td>
</tr>
<tr>
<td>Sales Representative</td>
<td>HR Assignment Status is Active</td>
<td>Sales Representative</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Salesperson</td>
<td></td>
</tr>
<tr>
<td>Sales Restricted User</td>
<td>HR Assignment Status is Active</td>
<td>Sales Restricted User</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Sales Restricted User</td>
<td></td>
</tr>
<tr>
<td>Sales Setup User</td>
<td>HR Assignment Status is Active</td>
<td>Application Implementation Consultant</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Sales Setup User</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>HR Assignment Status is Active</td>
<td>Sales VP</td>
</tr>
<tr>
<td></td>
<td>Resource Role is Sales Vice President</td>
<td></td>
</tr>
<tr>
<td>Contingent Worker</td>
<td>HR Assignment Status is Active</td>
<td>Contingent Worker</td>
</tr>
<tr>
<td></td>
<td>System Person Type is Contingent Worker</td>
<td></td>
</tr>
<tr>
<td>Employee</td>
<td>HR Assignment Status is Active</td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td>System Person Type is Employee</td>
<td></td>
</tr>
</tbody>
</table>

**Resource Roles and Provisioning Rules for Service**

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

These are the service role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles each rule provisions.
### Provisioning Rule Name | Condition | Job or Abstract Roles Provisioned
---|---|---
Service Vice President | HR Assignment is Active  
Resource Role is Service Vice President | Customer Service Manager  
Resource
Service Administrator | HR Assignment is Active  
Resource Role is Service Administrator | Customer Relationship Management  
Application Administrator  
Resource
Service Manager | HR Assignment is Active  
Resource Role is Service Manager | Customer Service Manager  
Resource
Service Representative | HR Assignment is Active  
Resource Role is Service Representative | Customer Service Representative  
Resource

**Note:** If you didn't use the Create Company Information quick setup task to set up your company information, then the predefined role provisioning rules aren't created; you must create the provisioning rules yourself. For information about creating provisioning rules, see the topic Create Rules to Automatically Provision Job Roles to Sales Users.

**Related Topics**
- Create Rules to Automatically Provision Job Roles to Sales Users

### Steps for Setting Up Role Provisioning

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

#### Create Additional Resource Roles

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

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

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

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

Create Additional Role Provisioning Rules

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

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

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

Related Topics

• Create Rules to Automatically Provision Job Roles to Sales Users
Get 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're getting ready to create two types of sales users:

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

Setup Overview

Before creating sales users, make sure that you 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 Create Additional Resource Roles.

2. Create a resource organization for each of the manager users you create, including the top manager in your hierarchy.
   You can use the Manage Internal Resource Organizations task to create each resource organization. For details, see the topic Create a Resource Organization. Alternatively, you can create each resource organization as you create each manager user in the UI or when you import the user. Individual contributors who aren't managers inherit the organization assigned to their managers.
   As you create users, the application creates an organization hierarchy that you can use to browse through the sales organization's resource directory.

3. You can explicitly designate the resource organization you create for the top manager in your organization as the top of your organization tree by using the Manage Resource Organization Hierarchies task. For details, see the topic Designate an Organization as the Top of the Sales Hierarchy.
   If you don't specify the top organization, the application automatically builds the resource organization hierarchy based on the management hierarchy you specify when you create users. You must enter a manager for each user you create, except for the manager at the top of the resource hierarchy.

4. Decide what job roles you want to assign to your users.
   Remember that you aren't restricted to assigning one job role to a user. For example, you might want to provision the sales manager in charge of 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 Create Rules to Automatically Provision Job Roles to Sales Users.

6. Enable duplicate checking for the email addresses you enter while creating users in the UI.

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

How Setup Assistant Gets You Ready to Create Sales Users

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

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

For information about the Setup Assistant, see the Getting Started with Your Sales Implementation guide.

Create a Resource Organization

Create a resource organization for every manager in your sales organization, including the top manager, usually the CEO. Use the procedure in this topic if you want to create your resource organization hierarchy before you create users. Alternatively, you can create resource organizations while you're creating manager users in the UI or when you import them. When you import users from a file, you can create the resource organizations automatically from the information you include in the file itself.

Creating the Resource Organization

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

2. On the Manage Internal Resource Organizations page, click the Create icon. The Create Organization: Select Creation Method page is displayed.

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

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

- Each resource organization name must be unique.
- The names don't have to correspond to any formal organization in your enterprise. The names are there solely to create a resource directory.
- Don't use the name of a manager as the organization name as you might want to reassign the organization to someone else later.

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

6. Click **Finish**.

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

**Related Topics**
- Update Existing Setup Data

---

**Designate an Organization as the Top of the Sales Hierarchy**

After you create the resource organization for the top person in the sales organization hierarchy, for example, the CEO, you can designate that resource organization as the top organization in the sales hierarchy. If you don't explicitly designate the top organization, the application automatically builds the resource organization hierarchy based on the management hierarchy you specify when you create users. You must enter a manager for each user you create, except for the manager at the top of the resource hierarchy.

**Designating the Top of the Sales Hierarchy**

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

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

2. On the Manage Resource Organization Hierarchies page, click **Search**.

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**
- Update Existing Setup Data

**Prevent Entry of Duplicate User Email Addresses**

You can prevent the entry of duplicate email addresses when creating or editing users on the Create User or Edit User pages by enabling email validation. The validation displays a warning message and lists the owner of the email address if you enter a duplicate value. Having this warning gives you the opportunity to enter a unique email before saving the user’s record. Email validation on the Create User and Edit User pages is disabled by default. Follow the steps in this topic to enable validation.

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

**Set the Profile Option**

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

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Sales Foundation
   - Task: Manage Administrator Profile Values
2. On the Manage Administrator Profile Values page, enter `PER_MANAGE_USERS_EMAIL_VALIDATION` in the Profile Option Code field and click Search.

3. In the Profile Values section of the search results, enter Y in the Profile Value field.

4. Click Save and Close.

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

Create Additional Resource Roles

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

Create a Resource Role

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

2. On the Manage Resource Roles page, review the existing resource roles by clicking Search without entering any search criteria.

   All the available resource roles are listed. Roles that are predefined by Oracle are labeled System.

3. To create a new resource role, click Create.

   The Create Role page appears.

4. In the Role Name field, enter the name of the resource role as you want it to appear in the application UI, for example, Digital Sales Manager.

5. In the Role Code field, enter a unique internal name in capital letters. No spaces are permitted but you can use the underscore character instead. For example, enter `DIGITAL_SALES_MANAGER`. If you’re importing users from a file then you must include this code in your file rather than the name.

6. If the resource role belongs to a manager, select the Manager option. If the resource role belongs to an individual contributor, select the Member option.

7. From the Role Type list, select Sales to classify the role that you’re creating.

8. Click Save and Close.

Related Topics

- Update Existing Setup Data
Create Rules to Automatically Provision Job Roles to Sales Users

Before you create sales users, review the predefined role provisioning rules used to automatically assign job and abstract roles to users, and create any additional rules you need. Oracle provides a role provisioning rule for each of the standard resource roles included with the application but you have to create role provisioning rules for any new resource roles you create. The provisioning rules use the resource role that you assign to each sales user as the trigger condition for provisioning job roles.

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

**Note:** The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. If you didn’t use the Create Company Information quick setup task, then you must create all of these role-provisioning rules manually. For information about the predefined provisioning rules, see the topic Role Provisioning. For information about setting up your company information, see the Getting Started with Your Sales Implementation guide.

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

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules

2. On the Manage Role Mappings page, if you want to review existing 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.
   b. Click Search.

      If a role provisioning rule exists for the resource role (either a predefined rule or a rule you created), it’s displayed in the Search Results area.
   c. To view or edit a provisioning rule, select the rule from the Search Results area.

      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 identifies the mapping. For example, if you’re creating a rule to provision a resource role you created called Digital Sales Manager, enter Digital Sales Manager for the mapping name too.

5. In the Conditions region, enter these conditions:
Get Ready to Create Sales Users

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

6. In the Associated Roles region, click Add to add the job roles you want to provision.
   For the Digital Sales Manager, for example, you might add the Sales Manager job role.
   For internal sales users, add the Resource abstract role. Don't add this role for partner roles.
7. Select one or more of the role-provisioning options shown in the table for each role you've added.

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

Qualifying users are users who satisfy the rule conditions.

**Note:** Autoproduction is selected by default. Remember to deselect it if you don't want autoproduction.

8. Click Save and Close.
9. Run the scheduled process Autoproduction Roles for All Users after creating or editing role mappings. This process compares all current user role assignments with all current role mappings and creates appropriate autoproduction requests.

**Related Topics**
- Update Existing Setup Data
- Role Provisioning

### Define Rules for Incentive Compensation Abstract Roles

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

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
To map the Incentive Compensation Participant Manager role:

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

**Role Provisioning Options**

Job and abstract roles are assigned to users by defining a relationship, called a role mapping or provisioning rule, between the role and some conditions. Users who satisfy the conditions defined in the rule are eligible to acquire the role or roles specified in the rule. Predefined provisioning rules are provided with the application but you can also create new rules using the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area. This topic describes role mapping options for automatic and manual role provisioning.

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

**Automatic Provisioning of Roles to Users**

Role provisioning occurs automatically if:

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

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

1. Specify these conditions for the rule:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Role</td>
<td>Digital Sales Manager</td>
</tr>
</tbody>
</table>
2. Specify the Resource abstract role and the Sales Manager job role for the provisioning rule, and select the Autoprovision option for each.

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

Manual Provisioning of Roles to Users

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

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

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

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

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

1. Specify these conditions for the rule.

<table>
<thead>
<tr>
<th>Field</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 these roles for the rule.

<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, when you assign the Sales Operations Manager resource role to a user, the user:

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

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

Role-Provisioning Rule Names

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

Role Autoprosioning

Autoprovisioning is the automatic allocation or removal of job or abstract roles to users. It occurs for individual users when you create or update the resource role assigned to a user or the user’s HR assignment status. You can also apply autoprovisioning explicitly for the enterprise using the Autoprovision Roles for All Users scheduled process. This topic explains the effects of applying autoprovisioning for the enterprise.

Roles That Autoprosioning Affects

Autoprovisioning applies only to roles that have the Autoprovision option enabled in a role mapping.

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

The Autoprovision Roles for All Users Scheduled Process

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

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

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

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

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

Autoprosion for Individual Users

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

Related Topics
- Schedule the Send Pending LDAP Requests Process

Provision Roles for Testing

What's Required for Testing Configurations in the Sandbox

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

What's Required for the Objects You Create

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

Setup Overview

1. While signed in as a setup user or the initial user you received when you signed up with Oracle, edit the role-provisioning rule for sales administrators and add the required job roles. Here is a summary of the steps:
   a. In the Setup and Maintenance work area, use the following:
      - Offering: Sales
      - Functional Area: Users and Security
      - Task: Manage HCM Role Provisioning Rules
b. Search for all role-provisioning rules containing the Sales Administrator job role.

c. For each rule, you add the job roles required for testing. Selecting the **Self-requestable** option makes it possible for individual users to assign themselves each job role when needed.

d. If you’re creating custom objects, then you must also add the Custom Objects Administration role. You must select both the **Self-requestable** and the **Autoprovision** option for this role. This object role is required for all objects you create, so you want to provision it automatically for future to sales administrators.

2. Sales administrators, who are resources with the Sales Administrator job role, navigate to the Resource Directory and assign themselves the job roles they need. Setup users, who are not resources, can edit their own user records in the Manage Users work area and assign themselves the roles there.

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

**Related Topics**
- Enter Setup Data Using Assigned Tasks

---

**Enable Sales Administrators to Test Configurations in the Sandbox**

Modify the security role-provisioning rules to make it possible for administrators to assign themselves the job roles they need for testing custom configurations in the sandbox. For viewing and testing the custom objects they create, administrators must have the Custom Objects Administration (ORA_CRM_EXTN_ROLE) role. To test job role-specific configurations, they must have the same job role. In this example, we are looking at sales administrators.

**Modify the Provisioning Rule for Sales Administrators**

1. Sign in as a **setup user** or the initial user you received when you signed up with Oracle.

2. In the Setup and Maintenance work area, use the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules

3. On the Manage Role Mappings page, search for the role mapping for sales administrators:
   - In the Search region, click the **Role Name** list and select the **Search** link.
   - In the Search and Select window, enter **Sales Administrator** in the **Role Name** field and click **Search**.
   - Select the role name and click **OK**.
   - 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:
   - In the Associated Roles region, click **Add Row** (the plus sign icon) and add the job roles required for testing.
   - For each job role, select the **Requestable** and the **Self-requestable** options and deselect **Autoprovision**. You don’t want the job roles assigned to the sales administrators automatically.
   - If you’re creating your own objects, then you must also add the Custom Objects Administration role. The application automatically generates this object role the first time you create an object. For this job role select all of the options: **Requestable**, **Self-requestable**, and **Autoprovision**. All users creating their own objects must have this role.
   - Click **Save and Close**.
6. When you have added the job roles to all the provisioning rules, click **Done**.

**Related Topics**
- Enter Setup Data Using Assigned Tasks

### Assign Yourself Additional Job Roles Required for Testing

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

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

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

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

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

The application returns you to the Resource page and displays the requested role in the Roles Requests region.

6. You can remove a role you no longer need for testing by selecting it and clicking **Remove**.
7. Click **Save and Close**.

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

### FAQs for Preparing for Application Users

**What happens when I autoprovise roles for a user?**

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

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

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

In a role mapping:
- The conditions specified for the role match the user’s assignment attributes, such as job.
- The role has the Autoprovision option selected.

Why can't I see the roles that I want to 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.

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

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

1. In Setup and Maintenance, go to the Manage Internal Resource Organizations task:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Internal Resource Organizations

2. You can search for the organization by name, or select Sales as the Usage for your search.
3. Edit the organization name and save your changes.
Create Sales Users

User Setup Options

There are a number of different options you can use to control default functionality when users are created in the application. You might have made decisions about user setup options when you configured your application security environment and set up the Security Console. But if you didn't, then it's a good idea to review the options described here and make any configuration changes you want before you start creating users.

User Name and Password Notifications

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

Password Policy

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

Default User Name Format

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

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

Related Topics

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

Create Application Users

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

This topic describes how to create individual sales users in the Manage Users task UI. If you have a large number of sales users to create, then importing users is useful. For additional information, see the chapter about importing sales users in the guide Getting Started with Your CX Sales Implementation. or the chapter about importing resource data in the guide Understanding Import and Export Management for CX Sales and B2B Service.
Before creating application users, make sure you have completed these tasks:

- 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’s a manager from the resource role you assign to the user.

When you create application users, you automatically set up the reporting hierarchy of your organization by indicating each person's manager. For this reason, first create the user at the top of the hierarchy and that user's organization. You don't enter a manager for this user. You can then create the rest of the users starting directly under the top of the hierarchy and working your way down.

Steps to Create an Application User

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

- You must assign each manager 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's a manager from the resource role you assign to the user.

1. Select Navigator > My Team > Users and Roles to open the Search Person page.
2. In the Search Results section, click the Create icon.

The Create User page opens.

3. In the Personal Details region, enter the user’s name and a unique email address. The application sends user notifications to this email address by default unless you disable notifications in the Security Console.

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

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

   If you’re planning to use quotas, then you must make sure that the hire date is a date before the start of the first quota period. For example, if you’re allocating monthly quotas for fiscal year July 01, 2015 to June 30, 2016, then you must enter a hire date of 7-1-2015 or earlier. You can’t change the hire date after you create the user.

5. In the User Details region, you can either create a new account or link an existing, standalone user account to the new person record you’re creating.
   - When creating Sales users, create a new account. To create a new account, select the *Enter user name* option and then enter a user name. If you leave the User Name field blank, then the user name is generated automatically using the enterprise default format. Unless you specify otherwise, email address is the default user name format.
   - Alternatively, if you want to link the new person record you're creating to an existing standalone user account, select the *Link user account* option, then search for and select the user account in the Link User Account dialog box.
6. In the User Notification Preferences region, select the **Send user name and password** option if you want a notification to be sent to the user when you save the user record and the user account is created. The notification includes a URL users can use to reset their password and sign in.

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

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

7. In the Employment Information region, enter the values shown in the following table.

<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’re 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’re creating is a manager, and if you already created a resource organization for this manager, then select the appropriate resource organization. If you haven’t created a resource organization for the manager, then you can create one by clicking the <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’re creating isn’t 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.

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

11. 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 user the email with the URL the user can use to sign in to the application for the first time.

13. Click **Done**.

**Related Topics**

- Create a Resource Organization
- Types of Sales Users

---

**Create 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.

Use these steps to create a sales restricted user.

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

2. When creating the user, specify these values.

<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 **Autoprovision Roles**.
The user is automatically assigned the following roles:

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

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

**Configure Administrators to Access Incentive Compensation**

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

1. Create provisioning rules that create a mapping between attributes of your person and the security role to be automatically assigned. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, enter a name for your mapping.
3. There isn’t a resource role that qualifies as an Incentive Compensation Administrator, so typically mappings use job roles. In the Conditions region, select a job role that was configured in Human Capital Management. For example, Incentive Compensation Analyst. Add any other conditions you want to use to select individuals to be assigned roles.
4. In the Associated Roles region, click **Add Row**.
5. Search for and select the role you want to assign to people who match your mapping conditions. These are the available Incentive Compensation roles:
   - Incentive Compensation Analyst
   - Incentive Compensation Plan Administrator
   - Incentive Compensation Manager
6. Save and close.
7. After users are assigned to an Incentive Compensation security role, they also need access to Incentive Compensation business units. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Incentives
   - Task: Manage Business Unit Data Access for Users
8. In the Manage Data Access for Users page, click **Create**.
9. Select a user name and role.
10. The security context must be Business Unit.
11. Select the name of the business unit in the Security Context Value field.
12. Save and close.
13. Create data access records for each role and business unit combination for this user.
14 User Management

Overview of Managing Users

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

- 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. But you can also use file import functionality to perform user management tasks such as:

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

For additional information, see the chapter about importing resource data in the guide Understanding Import and Export Management for CX Sales and B2B Service at http://docs.oracle.com.

Reset Passwords for Other Users

Use the Security Console to reset passwords for other users. Only setup users, and other users with the IT Security Manager job role, can access the Security Console. All users can reset their own passwords by clicking their user name or image, and selecting the Set Preferences link in the Settings and Actions menu. They can also reset their passwords by using Forgot Password on the sign-in page.

Use these steps to reset a user's password in the Security Console.

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

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

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

7. Click Reset Password.

**Related Topics**
- Update Existing Setup Data

### Change a User's Email Address

Use the Users tab in the Security Console work area to change email addresses for sales users. If you're updating their email addresses, 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:
   - First or last name, but not both
   - User name
4. Click the user name link.
5. On the User Account Details window, click Edit.
6. In the Edit User Account window, edit the email address.

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

7. Click Save and Close.

### Get User Sign-in Sign-out Information

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

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task Manage Administrator Profile Values.
2. Search the following Profile Option Code: ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the Profile Value drop-down list, select Yes.
4. Click Save and Close.
Note: The audit data is available for seven days.

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

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

### Change User Names

User names are automatically generated in the enterprise default format when you create a new user if you don't manually specify a user name. The default format is the user's email address, but you can change this value. For example, you might choose to use first name.last name as the default format. You can also manually override an individual user's existing user name, if necessary.

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

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

1. Select **Navigator > My Team > Users and Roles** to open the Search Person page.
   You can also search for the Manage Users task in the Setup and Maintenance work area.
2. Search for and select the user whose user name you want to change.
   The Edit User page for the user opens.
3. In the User Details region, enter the new user name in the **User Name** field.
   You can enter the user name in any format you choose.
4. Click **Save and Close**.
   The updated name is sent automatically to your LDAP directory server.
   The user's password and roles remain the same.

When you change an existing user name on the Edit User page, the user doesn't receive an automatic notification of the change. So it's a good idea to send details of the updated user name directly to the user.
Change 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 these 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 the resource import management functionality or using the Sales UI. Although importing changes takes care of many tasks that you have to perform manually in the UI, if you're updating resource role information for an individual user, then using the UI can be more efficient.

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

1. Sign in to the application as the sales administrator or as a setup user.
2. Select Navigator > My Team > Users and Roles to open the Search Person page.
3. Search for and select the user who's being promoted. The Edit User page for the user opens.
4. In the Resource Information region, do the following:
   a. In the Resource Role field, add the new resource role for the user, for example, Sales Manager.
   b. In the Reporting Manager field, update the user's manager.
   c. In the Organization field, specify the user's resource organization.
      You must create a resource organization for every manager in your Sales organization. If you haven't created a resource organization for the new manager, then you can create one by clicking the Create link from the end of the Organization list. The Create Organization dialog box is displayed allowing you to enter a new organization name.
   d. To automatically provision any roles provided by the new resource role you just assigned the user, click the Autoprovision Roles button in the Resource Information section.
   e. Click Save and Close.
5. Set an end date for the user's old resource role using these steps:
   a. Form the Navigator menu, select Directory > Resource Directory.
   b. In the Tasks area of the Resource Directory page, select View Resources.
   c. On the View Resources page, search for and select the user.
      The Resource page for the user opens.
      Note that the user is assigned the new resource organization you previously created.
   d. Click the Roles tab, and in the Roles list, select the current role assigned to the user, for example, Salesperson, and enter an end date in the To Date field.
      The value you enter is the date the user's assignment in the current role ends.
e. Click **Save and Close**.

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

For information about changing role assignments using the resource import management functionality, see the topic about importing resource data in the Understanding Import and Export Management for CX Sales and B2B Service guide.

**Related Topics**

- Import Your Resource Data

---

**View Locked Users and Unlock Users**

A user gets locked in the application either on entering incorrect password for multiple times or if the application hasn't been accessed for a certain period of time. The locked users report provides the list of locked users for both these scenarios.

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

**View Locked Users**

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

The spreadsheet shows the list of users who are locked.

The Locked Users spreadsheet contains the following two tabs:

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

**Unlock Users**

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

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

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

## Terminate User Accounts

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

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

The process outlined in this topic applies if you're using only Oracle CX Sales and B2B Service. If your company also uses Oracle HCM Cloud, then a different process applies.

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

### Inactivating a User Account

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

These are the steps to inactivate a user account.

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

### Removing Roles from a User

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

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

1. Navigate to the Search Person page as described in the previous task.
2. Search for and select the user whose roles you want to remove.

   The Edit User page for the user opens.
3. In the Current Roles section, select the role you want to remove, then click the **Remove** icon. Repeat this process for each role assigned to the user that you want to remove.

4. Click **Save and Close**.

---

### Setting an End Date for the Resource

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

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

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

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

2. On the Manage Resources page, search for and select the resource you want to edit. The Resource page for the individual opens.

3. With the Organization tab selected, select the **Edit** option from the **Actions** menu.
   - The Edit Organization Membership page opens.

4. In the **To Date** field, enter the date the individual is leaving the company.

5. Click **Save and Close**.

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

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

---

### Impersonation and Proxy Users

### Privileges Required by Proxy Users

You can use the impersonation functionality in the sales application 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 sign in to the Partner Portal as a partner user to resolve a query relating to the UI pages or data.

Channel managers don't 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**

- Impersonate a Partner User
- Copy Job or Abstract Roles

**Configure 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 enter the value of the Profile Value field to either Yes or No.
6. Click Save and Close.

**Provide Read-Only Access for Individual Users**

Some users may need read-only access to Oracle CX Sales and B2B Service applications. For example:
- A service representative must replicate a user’s transaction without saving any changes.
- An auditor reviews application data for regulatory reasons but isn’t authorized to change anything.

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

**Set the Read Only Mode Profile Option**

To enable read-only mode for a user:

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

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

**FAQs for Managing 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. But 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.
Can I reactivate a terminated employee record?

Yes. Once you specify an end date for a resource, you can’t reverse it in the application. But the former employee’s record remains in the application so you can again identify that person as a resource if the person is rehired. After identifying the person, you must assign roles and an organization again.

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

You can run the Send User Name and Password Email Notifications process in the Scheduled Processes work area. For users for whom you haven’t so far requested an email, this process sends out user names and reset-password links. The email goes to the work email of the user or the user’s line manager. You can send the user name and password once only to any user. A notification template for this event must exist and be enabled.
15 User and Role Reports

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 policies file is generated only when Data Security Policies is selected. <strong>Note:</strong> Extract the data security policies only when necessary, as generating this report is time consuming.</td>
</tr>
<tr>
<td>Any</td>
<td>Hierarchical</td>
<td>CSV</td>
<td>Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.</td>
</tr>
</tbody>
</table>
| • Multiple users  
  • All roles   | CSV         | CSV         | Functional security policies in a comma-separated, tabular format. |

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547 and the **Data Security Policies** option selected, then the report files are:

- ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip
- ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip
- Diagnostic.zip

**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**
- Schedule the Import User Login History Process

### 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
16 Review and Analyze Roles

Overview of Reviewing Roles

This chapter describes how you can 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 perform these 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 the privileges required for that access.
- Compare roles.
- Copy roles, create roles, and edit custom job, abstract, and duty roles.

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

From the Analytics tab, you can perform these tasks:

- 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.

Note: You can also use the Security Dashboard to get an overview of the security roles and how they’re provisioned in your environment. For information, see the topic describing the Security Dashboard in this chapter.

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:
  o If **Expand Toward** is set to **Privileges**, then you can set **Show** to either **Privileges** or **Roles**.
  o 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.

### Review 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.

Simulate Navigator Menus

You can simulate the Navigator for both users and roles. This feature can help you to identify how access is provided to specific work areas and tasks. You can then use this information when creating roles, for example.

Simulate the Navigator for a Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the role, which can be of any type.
2. In the search results, select Simulate Navigator in the Actions menu for the role. The Simulate Navigator page opens. Icons may appear against Navigator entries. In particular:
   - The Lock icon indicates that the role can't access the entry.
   - The Warning icon indicates that the entry may not appear in the Navigator as the result of configuration, for example.

   Entries without either of these icons are available to the role.

   Tip: To view just the entries that the role can access, set Show to Access granted.

View Roles That Grant Access to a Navigator Entry

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the roles that grant access. Follow these steps:

1. Click the entry.
2. Select View Roles That Grant Access.
3. In the Roles That Grant Access dialog box, review the list of roles. The roles can be of all types. After reviewing this list, you can decide how to enable this access, if appropriate. For example, you may decide to provision an abstract role to a user or add a duty to a custom role.
4. Click OK to close the Roles That Grant Access dialog box.

View Privileges Required for Menu

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the privileges that grant access to:

- The Navigator entry
- Tasks in the associated work area

Follow these steps:

1. Click the entry.
2. Select View Privileges Required for Menu.
3. In the View Privileges for Work Area Access dialog box, review the list of privileges that grant access to:
   - The Navigator menu item.
   - Task panel entries in the associated work area. In the **Access Granted** column of this table, you can see whether the selected role can access these tasks.

You can use this information when creating roles, for example. You can identify how to both add and remove access to specific tasks and work areas.

4. Click **OK** to close the View Privileges for Work Area Access dialog box.
5. Click **Close** to close the Simulate Navigator page.

### Simulate the Navigator for a User

Search for the user on the Roles tab of the Security Console and select **Simulate Navigator** in the **Actions** menu for the user. Follow the instructions for simulating the Navigator for a role.

### Review 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.

#### View 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.

#### Identify 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.

Compare 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 isn’t 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
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’re adding the policies. This must be a custom role. You can’t 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.

### Compare Users

You can compare users to identify their access permissions and assign the missing permissions as required. This comparison includes both direct and inherited roles. From the results, you can find out if there are any discrepancies in roles.

Only administrators with the View User Account (ASE_VIEW_USER_ACCOUNT_PRIV) privilege can compare users. On the User Accounts page, you can compare users in two different ways:

- Use the Compare Users button.
- Search for a user and then click Compare Users from the Actions menu of that user.

Follow these steps:

2. Click Compare Users.
3. Search for and select both users one after another.
4. Click Compare. All the details of both the users are displayed.

In the comparison results, you can do the following actions:

- Click one of the Show options to view the corresponding details in the results.
• Click the Query By Example icon to enter the name of a specific role that you want to see from the search results.

You can then use the Export to Excel option to export the filtered search results.

Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance.

On the Analytics page, click the Roles tab. 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:

  o Roles
  o Role memberships (roles belonging to other roles within the category)
  o 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:

  o Role memberships
  o Security policies
  o Users assigned to 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.

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.

1. On the Analytics page, click the Database Resources tab.
2. Select the resource you want to review in the Database Resource field.
3. 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 comprise the following:

- 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 following:

- 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 do the following actions:

- 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.
View Role Information Using Security Dashboard

As an IT Security Manager, you can use the Security Dashboard to get a snapshot of the security roles and how those roles are provisioned in the Oracle Cloud Applications. The information is sorted by role category and you can view details such as data security policy, function security policy, and users associated with a role. You can also perform a reverse search on a data security policy or a function security policy and view the associated roles.

You can search for roles using the Role Overview page. You can view the count of the roles which includes the inherited roles, data security policies, and function security policies on this page. Clicking the number in a tile on this page takes you to the corresponding page in the Role Dashboard. You can view role details either on the Role Overview page of the Security Dashboard or the Role Dashboard.

You can view role information such as the directly assigned function security policies and data security policies, roles assigned to users, directly assigned roles, and inherited roles list using the Role Dashboard. Clicking any role-related link on a page of the Security Dashboard takes you to the relevant page in the Role Dashboard. You can export the role information to a spreadsheet. The information on each tab is exported to a sheet in the spreadsheet. This dashboard supports a print-friendly view for a single role.

Here are the steps to view the Security Dashboard:

1. In the Reports and Analytics work area, click Browse Catalog.
   All pages of the dashboard are listed.
3. To view the Role Category Overview page, click Open.
   The page displays the number of roles in each role category in both tabular and graphical formats.
4. In the Number of Roles column, click the numeral value to view the role-related details.
5. Click View Role to view the role-specific information in the Role Dashboard.
17 Create and Edit Job, Abstract, and Duty Roles

Overview of Security Configuration

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. 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.

This chapter describes how you can create your own roles and role hierarchies. For information about configuring data security, see the chapter Configure and Troubleshoot Data Security.

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.

Related Topics

• Overview of Data Security Configuration

Guidelines for Copying Roles

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 can't copy roles that are used to secure sales analytics and reports. Therefore you can't 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. When you create a custom job role, either from scratch or by copying an existing job role and editing it, make sure that the role is assigned the BI Consumer role and BI Author role if the custom role is to provide access to analyses and reports. The BI Consumer role provides view-only access to analyses and reports; the BI Author role provides access to create and edit analyses and reports.

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

- Role Preferences

Copy 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.

Edit 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).
Create and Edit Job, Abstract, and Duty Roles

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.

Create 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 **Digital Sales Manager**.
3. Enter a unique **Role Code** value. For example, enter **DIGITAL_SALES_MGR_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're not 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.
6. Close the **Add Function Security Policy** dialog box.

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're 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.

Copy and Edit 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.
   o 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.
   o 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.
6. Close the **Add Function Security Policy** dialog box.
7. All the privileges you selected are listed on the Edit Role: Function Security Policies page.
8. 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.

### Edit Data Security Policies on the Security Console

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

### 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:
   - To remove the policy, select the **Remove Data Security Policy** option.
     - The policy is removed from the role.
   - To edit the policy, do the following:
     1. Select the **Edit Data Security Policy** option.
        - The **Edit Data Security Policy** dialog box is displayed.
     2. Change the values as required, for example, you can change the start date, the data set, or the action specified for the policy.
     3. 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>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>All values</td>
<td>Use to include all data from the data resource in the data set.</td>
</tr>
</tbody>
</table>
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.
Overview of Data Security Configuration

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

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 isn't on the opportunity team. The scope of visibility varies by object and multiple visibility levels are supported by an object for a role.

You can configure data security using the Sales and Service Access Management work area or the Security Console. In general, use the Sales and Service Access Management work area to review, configure, and troubleshoot data security. But 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. Both types of tasks are described later in this chapter.

Note: Data security changes made in either work area are immediately available in both work areas.

Sales and Service Access Management Work Area

As an IT Security administrator, you must be able to easily view the data a predefined role can access and to easily configure access to data for a user group using custom roles. Administrators must also be able to troubleshoot access issues for users. You can perform all of these tasks using the Sales and Service Access Management work area, which provides simple interfaces where you can do these tasks:

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

- Troubleshoot access issues for users:
  - Review a user's access to object data
  - Identify the cause of any issues the user is experiencing in accessing specific records

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

See the Access Groups chapter for information about using access groups.
**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.

### Review and Configure Data Access for Roles

#### Review a Role's Access to Object Data

You can review the visibility provided by job roles to object data 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 answer questions such as these:

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

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

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

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

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

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

4. Select an object in the **Object** field.
The **Object** field lists all the sales and service objects the role can access.

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

5. Click **Find Policies**.

The Access Policies table now lists all the active data security policies relating to the object you selected, such as Trading Community Party, 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.

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

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

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

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

a. Select **Sales Representative** in the Role field, **Trading Community Party** in the Object field, and click **Find Policies**.

b. Click the **Query By Example** filter icon, and enter the text **All records** in the query field above the Condition column.
The page is refreshed and displays two policies that provide all record access. Notice that one policy is provided by the Sales Representative role and the other by an inherited role, Contract View Access Across All Contracts. If you wanted to create a version of the Sales Representative role that had more restricted access to accounts and contacts, you would have to create custom copies of both roles and remove the All records policies from each.

To remove the filter, click the Clear All icon in the query row.

7. To view the advanced permissions defined for a selected policy in the Access Policies table, scroll to the Advanced Permissions table.

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

For each advanced permission, the Advanced Permissions table shows the type of access provided, for example, Read access, and the action it relates to, for example, View Opportunity.

8. If you want to view the inactive policies for a selected role and object on the Sales and Service Access Management page, then select the Inactive policies check box.

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

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

You can update existing and future-dated policies for a custom role and object, and grant access to new subsets of 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

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

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.
2. Select Navigator > Tools > Sales and Service Access Management.
   The Sales and Service Access Management page is displayed.
3. Search for or select a role in the Role field.
   You can't edit policies on predefined roles, so search for and select a custom role. For example, if you copied the predefined 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.
   Note: Select the Trading Community Party object to view access policies for both accounts and contacts.
5. Click Find Policies.
6. Click the Edit icon and the Active Policies edit page for the selected role and object is displayed.
The Access Policies table shows all available policies for the selected role and object by default but you can use the **Show Conditions** filter to display only policies that are granted or only policies that are not granted.

7. 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.

8. You can remove all access granted by a policy. For example, if your company doesn't use territory access, you can remove territory access to lead data using one of the following methods:

- Review the 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're no longer active by selecting a date that has passed in the **End Date** field, for example, select yesterday's date.

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

9. 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 isn't selected, none of the read permission options in the Advanced Permissions table can be edited.

10. 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.

---

**Considerations When Editing Inherited Roles**

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

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

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

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

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

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

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

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

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

**Edit Inactive Policies**

If you specified an end date for a policy, then once the end date is passed, the policy is inactive. You 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 Find Policies.
All inactive policies are displayed in the Access Policies table.

4. Click the **Edit** icon.

5. On the Inactive Policies page, select a policy and click the **Delete** icon.

6. Click **Yes** when a warning is displayed.

7. 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.

---

## Extend Access to Additional Objects for a Custom Role

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

For example, if you want to provide sales managers with access to 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, click the **Create** button.

2. On the Create Policies page, search for the custom role whose access you want to extend in the **Role** field.

3. 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.

4. Click **Find Policies**.

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

5. Locate the condition that provides the data access you want to implement for the object.

   For example, if you want to provide the custom sales manager role with read access to all 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**.

6. 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.
Note: You can view data security for custom objects using the Sales and Service Access Management work area, but you can only edit security policies for custom objects using Application Composer.

Review and Troubleshoot Data Access Issues for Users

Overview of the Data Access Explorer

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

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

To identify the cause of a user access issue, you must be able to view the data access policies that a user is currently granted for an object, and all the policies that provide access to the relevant object or record. You can view both types of information on the Explore UI. You can:

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

With this information, you can identify why a user can or can't view a specific record or records, and then grant or revoke the appropriate data security policies using the Sales and Service Access Management UI.

Make Additional Objects Available in Access Explorer

You can view a user's data access to the following objects by default on the Explore UI:

- Opportunities
- Leads
- Activities
- TCA Party

If you want to be able to view user access to additional objects, you can do so by configuring the lookup, Enable Staged Object Access in Access Explorer, and specifying lookup codes for each object you want to make available. This procedure describes what you need to do to expose additional objects on the Explore page.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Sales Foundation
   - Task: Manage Standard Lookups
2. On the Manage Standard Lookups page, create a lookup type with the following values:
   - Lookup Type: ZCA_SAM_STAGED_OBJECT_ACCESS
   - Meaning: Enable Staged Object Access in Access Explorer
   - Module: Simplified Access Management

3. Click **Save**.

4. Create lookup codes for each object you want to make available on the Explore page. For example, to add two partner objects as lookup codes, enter these values.

<table>
<thead>
<tr>
<th>Lookup Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZPM_PARTNER_PROFILES</td>
<td>Partner Profile</td>
</tr>
<tr>
<td>ZPM_PROGRAM_ENROLLMENTS</td>
<td>Partner Program Enrollment</td>
</tr>
</tbody>
</table>

5. Click **Save and Close**, then click **Done**.

**Object Lookup Codes**

This table shows the lookup code to specify for each object you can expose on the Explore page.

<table>
<thead>
<tr>
<th>Object Lookup Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HZ_CUST_ACCOUNTS</td>
<td>Trading Community Customer Account</td>
</tr>
<tr>
<td>MKL_DM_DEAL_PRODS</td>
<td>Deal Registration Product</td>
</tr>
<tr>
<td>MKL_DM_DEAL_RESOURCES</td>
<td>Deal Registration Team</td>
</tr>
<tr>
<td>MKL_DM DEALS</td>
<td>Deal Registration Summary</td>
</tr>
<tr>
<td>MKT_BDT_BDGT_ENTRIES</td>
<td>Marketing Budget Entry</td>
</tr>
<tr>
<td>MKT_BDT_BUDGETS_B</td>
<td>MDF Budget</td>
</tr>
<tr>
<td>MKT_BDT_CLAIMS</td>
<td>MDF Claim</td>
</tr>
<tr>
<td>MKT_BDT_CLM_SETTLEMENTS</td>
<td>MDF Claim Settlement</td>
</tr>
<tr>
<td>MKT_BDT_FUND_REQUESTS</td>
<td>MDF Request</td>
</tr>
<tr>
<td>MKT_CM_CAMPAIGNS</td>
<td>Top Level Campaign</td>
</tr>
<tr>
<td>Object Lookup Code</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>MKT_IMP_MAP</td>
<td>File Import Mapping</td>
</tr>
<tr>
<td>MKT_IMP_OBJECTS</td>
<td>File Import Object</td>
</tr>
<tr>
<td>MOT_TERR_PROPOSALS</td>
<td>Sales Territory Proposal</td>
</tr>
<tr>
<td>MOT_TERRITIES</td>
<td>Sales Territory</td>
</tr>
<tr>
<td>OSS_SUBSCRIPTIONS</td>
<td>Subscription</td>
</tr>
<tr>
<td>SVC_SERVICE_REQUESTS</td>
<td>Service Request Header</td>
</tr>
<tr>
<td>SVC_WORK_ORDERS</td>
<td>Field Service Work Order</td>
</tr>
<tr>
<td>ZCA_ASSET</td>
<td>CRM Asset</td>
</tr>
<tr>
<td>ZCA_BP_BUSINESS_PLANS</td>
<td>Sales Business Plan</td>
</tr>
<tr>
<td>ZCA_OBJECTIVES</td>
<td>Sales Objective</td>
</tr>
<tr>
<td>ZCA_SALES_ORDER_HEADERS</td>
<td>Sales Order</td>
</tr>
<tr>
<td>ZPM_PARTNER_PROFILES</td>
<td>Partner Profile</td>
</tr>
<tr>
<td>ZPM_PARTNER_PROGRAMS_B</td>
<td>Partner Program</td>
</tr>
<tr>
<td>ZPM_PROGRAM_ENROLLMENTS</td>
<td>Partner Program Enrollment</td>
</tr>
</tbody>
</table>

Review a User's Access to Object Data

You can view all the policies that currently affect the visibility a user has to an object, and the names of all the roles that provide each policy, using the Sales and Service Access Management access explorer functionality.

A user can be granted the same data access policy from more than one role. For example, a user might be granted a policy directly by a job role, and indirectly by a duty role that the job role inherits. Being able to identify all the roles that provide a policy to a user is essential when you want to remove a user's access to a set of data.

Use these steps to review all the policies that affect a user's access to an object.

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

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

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

5. Click the **Explore** button.

All the currently active policies for the object that are granted directly or indirectly to the user are displayed. For each policy you can also view:

- The name of the role that provides the policy. If the user inherits the policy from more than one role, click the link beside the role name to see a list of all roles.
- The status of the policy. By default, active policies are displayed.
- The policy start and end dates, and the permissions provided by the policy.
- Whether or not the policy condition is a custom condition.

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

You can display more or less data for each policy by selecting options from the **View** menu.

6. Once you have reviewed all the active policies assigned to the user, you can select options from the **Show Conditions** drop-down list to view other policies available for the object. This table shows the options available.

<table>
<thead>
<tr>
<th>Filter Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Display all policies defined for the object, including policies that are granted to the user and policies that aren't granted.</td>
</tr>
<tr>
<td>Granted and active</td>
<td>Display all active policies for the object that are granted to the user. This is the default value.</td>
</tr>
<tr>
<td>Granted and inactive</td>
<td>Display all inactive policies defined for the object that are granted to the user.</td>
</tr>
<tr>
<td>Granted and future dated</td>
<td>Display all inactive policies defined for the object that are granted to the user which are set to become active at some date in the future.</td>
</tr>
<tr>
<td>Not granted</td>
<td>Display all policies defined for the object that aren't currently granted to the user.</td>
</tr>
</tbody>
</table>
Troubleshoot a User Access Issue

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

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

For example, the predefined Sales Manager role allows sales managers to view the opportunity records belonging to their subordinates. If a manager reports that she can't see the opportunities of one of her subordinates, use the Explore page to discover what's causing the problem. To do this, you need the following information:

- The user name of the manager
- The object name, in this case, opportunity
- The Public Unique Identifier of one of the subordinate user's opportunity records

When you enter this information on the Explore page, all the policies that give access to the record are listed. You can then check if the manager is provisioned with these policies, identify the role providing the policy, and update the role to grant the policy.

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

1. Select Navigator > Tools > Sales and Service Access Management.
3. On the Explore page, select the name of a user in the User Name field. In this scenario, enter the name of the sales manager.
4. Select an object in the Object field. In this scenario, select the Opportunity object.
5. Enter the PUID of one of the opportunity records that the manager wants to access in the Public Unique Identifier field.
   For information on how to find the PUID of a record, see the topic Display the Public Unique Identifier for Object Records.
6. Click the Explore button.
   All the access policies for the object that grant access to the record are displayed by default.

The Status field shows whether or not each policy is granted to the user whose name you selected in the User Name field. The Status column can have one of these values:

- Active: The policy is active and is granted to the user.
- Inactive: The policy is granted to the user but is inactive.
- Future Dated: The policy is granted to the user but is not yet active.
- Not Granted. The user is not granted the policy.
The **Provides Record Access** field indicates whether or not an individual policy grants access to the record specified in the **Public Unique Identifier** field. A check mark in the field indicates that the policy provides record access; if the field is empty, the policy doesn't provide access to the record.

You can use the information from the **Status** and **Provides Record Access** fields to figure out what you have to do to provide the user with access. For example, you might find that the policy that provides a sales manager with access to their subordinates opportunity records is future dated. In this case, note the name of the role providing the policy and edit the role on the Sales and Service Access Management page to change the start date of the policy to the current date.

7. By default, the value of the **Show Conditions** drop-down list is **All** and the value of the **Provides Record Access** drop-down list is **Yes** so the Explore page lists all policies defined for the object that grant access to the record.

You can change the selections in these lists to provide different views of the user's access to object data. For example, to view all the policies that are defined for the object, including policies that do and policies that don't provide access to the record, select **All** from the **Show Conditions** list and leave the **Provides Record Access** drop-down list empty.

### Display Public Unique Identifiers for Object Records

The sales application generates a unique number (or ID) for each business object record, such as an opportunity record, when the record is created in the database. As an administrator, you can configure the unique ID that's generated to make it more user-friendly and readable. This user-friendly value is called the public unique ID (PUID).

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

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

1. Activate a sandbox. See the topic Create and Activate Unified Sandboxes for more information.
2. Select **Navigator > Configuration > Application Composer**.
3. On the Application Composer Overview page, navigate to the standard object whose PUID values you want to expose.
   For example, expand **Opportunity**
4. Select the **Pages** node.
5. Select the Application Pages tab.
   You can use the links on the tab to navigate to the object's configuration pages, where you can modify the pages that are available for the selected object. You can show or hide fields, rearrange fields, and add your own fields.
6. The **Opportunity Number** field shows the PUID value for an opportunity record. To make this field available on the UI, in the Landing Page Layouts region, select Standard Layout, then select **Duplicate** from the **Actions** menu.
7. Enter a name for the new layout, then click **Save and Edit**.
8. Locate the Fuse Opportunity Overview Table area and click the **Edit** icon.
9. In the Available Fields list, locate the **Opportunity Number** field and move it to the Selected Fields list.
10. Click Save and Close.
11. Test the changes by navigating to the Opportunities page as a user with access to the opportunities pages, for example, a salesperson.
12. Search for an opportunity, and verify that the PUID value is showing for the opportunity.
13. Publish the sandbox.
14. Navigate to the Sales > Opportunities page and search for an opportunity record. The PUID of the opportunity is displayed.

For information on exposing attributes and working with sandboxes, see the Oracle Applications Cloud Configuring Applications Using Application Composer guide. For information on public unique IDs, see the Oracle CX Sales Implementing Sales guide.

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

<table>
<thead>
<tr>
<th>Object Name in Application Composer</th>
<th>PUID Field to Expose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Registry ID</td>
</tr>
<tr>
<td>Activity</td>
<td>Activity Number</td>
</tr>
<tr>
<td>Asset</td>
<td>Asset Number</td>
</tr>
<tr>
<td>Business Plans</td>
<td>Number</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Campaign Number</td>
</tr>
<tr>
<td>Contact</td>
<td>Registry ID</td>
</tr>
<tr>
<td>Deal Registration</td>
<td>Registration Number</td>
</tr>
<tr>
<td>Deal Registration: Deal Products</td>
<td>DealProdNumber</td>
</tr>
<tr>
<td>Deal Registration: Deal Resources</td>
<td>DealResourceNumber</td>
</tr>
<tr>
<td>MDF Budget</td>
<td>Code</td>
</tr>
<tr>
<td>MDF Claim</td>
<td>Code</td>
</tr>
<tr>
<td>MDF Claim Settlement</td>
<td>Code</td>
</tr>
<tr>
<td>MDF Request</td>
<td>Code</td>
</tr>
</tbody>
</table>
Manage 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.

Define Database Resources

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

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

Create Conditions for a Database Resource

Database resource conditions define what portions of a database resource can be secured by data security policies. You can’t edit the predefined conditions provided by Oracle but you can create new conditions for a predefined database resource or for a database resource you 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>
<tr>
<td></td>
<td>If you specified the Tree Operators option, click the Search icon. The <strong>Select Tree Node</strong> dialog box is displayed allowing you to choose the operator value.</td>
</tr>
</tbody>
</table>

   - 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**.
19 Access Groups

Overview of Access Groups

Use access groups to provide sales resources with additional access to sales object data. Access groups are an alternative way of granting data permissions to users, and they use a different access path to that provided by the predefined data security policies.

An access group uses the access control list model. You create an access group, assign users to the access group and all group members are given access to standard or custom object data. You define object sharing rules which provide users with access to the specific records of an object. These rules specify the type of access to an object to be provided and the conditions under which the access is provided. For example, users might be granted access to:

- All opportunities with a status of Open
- All accounts where country is set to UK

You can also define the type of data access provided, for example, Full access or Read access.

A user can be assigned to one or more access groups and will have the access assigned to each group. So if Lisa Jones is assigned to Access Group A, which provides access to opportunities, and Access Group B, which provides access to Accounts, she receives the access provided by both groups. You can also use one access group to assign access to multiple objects.

Objects Supported for Access Groups

You can create access groups to provide data access to these objects:

- Account
- Activity
- Asset
- Business Plan (includes Sales Objective)
- Campaign
- Contact
- Contests
- Custom objects
- Deal Registration
- Duplicate Resolution Request
- Forecast Territory Details
- Household
- MDF Budget
- MDF Claim
• MDF Request
• Note
• Opportunity
• Partner
• Program Enrollments
• Resource
• Sales Lead
• Sales Orders (Quotes and Orders)
• Sales Quota Plan
• Sales Resource Quota
• Sales Territory
• Sales Territory Proposal

Access Group Privileges

Users assigned the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV) can create and manage access groups. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege. If you use custom versions of these roles, assign this privilege to your custom roles.

Resource users must be assigned a duty role, the Access Groups Enablement role, to be added as members of access groups. By default, users assigned any of these roles have this privilege:

• Resource abstract role
• Partner Sales Representative job role
• Partner Sales Manager job role
• Partner Administrator job role

If you use custom versions of these roles, assign the Access Groups Enablement duty to your custom roles.

Caution: Don’t make any changes to the predefined data security policies assigned to the Access Groups Enablement duty role. Changing or deleting these data security policies prevents the access groups functionality from working correctly.

How Access Groups Work with Other Security Mechanisms

You use access groups to supplement the data access users receive through their job roles and other security mechanisms. So when you configure users visibility to data using access groups, keep in mind that if you want only the access path provided by the group membership to take effect, you might also have to remove the access granted to group members by custom or predefined data security policies. If you don’t remove these other access paths, users will have the data visibility granted both by the access group, and by existing data security policies they’re assigned through record ownership or team membership, or through territory management setup.
Example of How Access Groups Interact with Other Security Mechanisms

The following example illustrates how the different security mechanisms work together.

Let's say Lisa Jones, who's assigned the Sales Representative job role, requires access to all opportunities in Germany for a specific project. Currently, Lisa can only access a subset of German opportunities through her team and territory membership. Lisa's manager, Mateo Lopez, doesn't need access to the additional opportunities in Germany.

To provide Lisa with the additional access she needs, do the following:

1. Create an access group and add Lisa Jones as a member of the group. Don't add Mateo Lopez to the group.
2. Create an object sharing rule for the access group that includes a condition similar to the following:

   Access all opportunities where country = Germany

Lisa can now access all opportunities in Germany. What opportunities can Mateo now access? Mateo Lopez isn't a member of the access group, and access groups don't provide access through the resource hierarchy by default, so Mateo can't access the additional opportunities in Germany through Lisa's access group membership.

Lisa's manager can only access opportunities through the resource or territory hierarchy where Lisa is on the sales team, the account team, or the territory associated with the opportunity.

- If Lisa isn't on the team or territory of the opportunities that she gets access to through her access group membership (all opportunities in Germany), then Mateo still can't access those opportunities.
- If Lisa is on the team or territory of some of the opportunities in Germany, then both Mateo and Lisa have access to that subset of opportunities through the standard security mechanisms, regardless of Lisa's access group membership.

Access Groups and Functional Privileges

You can use access groups to give users additional permissions at the data security level. You can't use access groups to provide functional security access privileges. Consider the example of a user assigned a job role which provides the functional privilege to view leads, but not the functional privilege to delete them. If you assign the user to an access group that specifies rules that provide delete lead and view lead data access, the user will be able to view leads but without the delete functional privilege, they still won't be able to delete leads.

Considerations in Deciding When to Use Access Groups

You can extend a user's visibility to sales object data in a number of ways:

- By creating custom data security policies, assigning the custom policies to custom roles, and then assigning the custom roles to users.
- By using Territory Management to set up territories and to assign users to territories, then using Assignment Manager to assign territories to object records.
- By creating access groups and assigning users to the access group.

So what factors should you consider when deciding which option to choose? This topic provides you with some guidelines.
Custom Data Security Policies

In situations where you can use either access groups or custom data security policies to provide users with data permissions, use access groups for these reasons:

- Access groups provide better performance than custom data security policies.
- You can search for records assigned to users through their access group membership in Workspace. Records assigned to users through custom data security policies can't be searched in Workspace.
- Access groups are easier to manage.

Access Groups

Access groups work together with the existing access mechanisms to allow you to provide access to users based on parameters that aren't provided by the standard access framework, such as the user’s context (country or sales region for example), the user’s resource organization or business unit, or some other attribute. You can also use access groups to assign access based on custom attributes. For example, you can assign all users in a specific business unit to a group and then grant that group read permissions to opportunities.

 Territory Management

You can use territory management to manage users visibility to data but territory management isn’t a security access mechanism. It's a way of assigning sales representatives to sales territories to enable optimal sales coverage. Territory management is used for configuring access primarily to facilitate the selling process by defining boundaries using hierarchical attributes such as products, geographies, industry and so on.

Use territory management functionality to extend visibility to data in these scenarios:

- If you want to use forecasting or quota management functionality.
- If the territory hierarchy and territory based reporting and roll-ups are different to the reporting resource hierarchy.
- If you want to provide users with access based on hierarchical attributes and named accounts.

If you want to provide users with access using a standard mechanism, such as territory or management hierarchy, then use Territory Management. Otherwise, use access groups.

Note: Once you’ve implemented territory management, you can optionally use access groups to manage your territories. You can define custom rules for the Sales Territory or Sales Territory Proposal objects and assign them to custom access groups to specify who can manage the territory or territory proposal. For example, you can create rules for country-specific administrator access groups that allow the group members to view all territories in their country but not edit or delete the territories.

Types of Access Groups

There are two types of access groups:

- Custom access groups.
Custom access groups are groups you create to provide users with access to data according to the needs of your business. You can add members to these groups, define rules to specify the access group members should have to object data, and edit or delete the groups as required.

- System access groups.

These are access groups Oracle creates for you. A separate group is created for each of the predefined job roles in your environment and for the Resource abstract role. Predefined object sharing rules associated with each group provide the same access to data as is provided by the predefined job roles. These rules are inactive by default.

A system access group is also created for each of the custom job roles in your environment but these system groups aren't associated with predefined rules; you can manually add predefined or custom rules to these system groups as required.

You can’t edit, create, or delete system access groups. You also can’t add members to or delete members from these groups. Users are automatically added to or removed from system groups according to the job roles they're assigned.

On the Access Groups UI, the **Type** field indicates whether a group is a system group or a custom group. Custom groups are displayed by default but you can choose the type of group you want to view from the **List** drop-down list.

### Overview of the Access Groups UI

You create and manage access groups and object sharing rules using the Access Groups UI in the Sales and Service Access Management work area. The Access Groups UI includes 2 tabs: the Access Groups tab and the Object Sharing Rules tab. Choose the appropriate tab depending on what you want to do:

- **Access Groups tab**
  
  Displays the main Access Groups page. From here, you can review all the existing custom or system access groups, you can create custom access groups, review or add group members, and review or enable the rules assigned to a group. You can also add new rules to a group.

- **Object Sharing Rules tab**
  
  Displays the main Object Sharing Rules page. From here, you can review all the rules defined for a selected object, you can create or delete object sharing rules and access extension rules, and you can assign rules to access groups.

You can manage your groups and rules on an on-going basis using either UI, depending on whether you want to work with access groups from an access group context or an object sharing rules context. For example, reviewing rule information from a rules context is useful if you decide to delete an object sharing rule you previously created and want to first check the rule isn't assigned to active groups. Similarly, reviewing rule information from a group context is useful if, for example, you want to enable and activate all the predefined rules assigned to a specific system group.

### Create and Manage Custom Access Groups
Create a Custom Access Group

This topic guides you through the main steps in the process of creating an access group and providing group members with access to object data. It describes these tasks:

1. Create an access group
2. Create object sharing rules to give group members access to object data
3. Add members to the group

More detailed information about each task is available in other topics in the chapter.

**Note:** You must be assigned the IT Security Manager job role or the Sales Administrator job role to create and manage access groups.

**Step 1. Create an Access Group**

Once you have identified a group of resource users that require additional access to object data, create an access group for those users.

1. Sign in to the application as the sales administrator or as a setup user.
2. In the Setup and Maintenance work area, go to the following:
   a. Offering: Sales
   b. Functional Area: Users and Security
   c. Task: Manage Sales and Service Access

   Alternatively, click **Navigator > Tools > Sales and Service Access Management**.

   If you're a Sales Administrator, the Access Groups page in the Sales and Service Access Management work area is displayed.

3. If you have the IT Security Manager job role, the Sales and Service Access Management main page is displayed. Click **Configure Groups** to display the Access Groups page.

   The Access groups page lists any existing active access groups. You can view all access groups (active and inactive) by selecting **All Groups** from the List drop-down list. You can also search for an existing group on this page.

4. Click **Create Access Group** to display the Create Access Group page.

5. Enter these values for the new access group.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for your group. For example, if you're creating a group to give sales support users access to all open opportunities, you might name the group <strong>Opportunity_Open</strong>.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for your group (optional). For example, <strong>Access to open opportunities</strong>.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Select a status for the new group. By default, the status for new groups is inactive. Click the <strong>Active</strong> check box to activate the group.</td>
</tr>
</tbody>
</table>

6. Click **Save and Continue** to save your new group.
Step 2. Create Object Sharing Rules for the Group

Next, create object sharing rules to grant group members access to object records.

2. To create a new rule, click **Create Rule**.
3. On the Create Object Sharing Rule page, select the object you’re creating the rule for from the **Object** dropdown list. For example, select **Opportunity**.
4. Enter a **Name** for your new rule, for example, **Opportunity_Open**. You can optionally enter a rule **Description**.
5. In the **Access Level** field, select the type of object access you want to give group members, either **Read**, **Update**, **Delete** or **Full** access.
6. Make sure that the **Active** check box for the rule is checked.
7. In the **Conditions** area, specify the rule conditions.
   For example, you might specify that group members have access to opportunity records that have a **Status** attribute equal to **Open**.
8. Select **Save and Publish** from the **Actions** menu to make the new rule available for assignment processing.
9. When the status indicator shows the publish process has completed, select **Save and Close** from the **Actions** menu.
10. Now run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the object sharing rules for each object are assigned properly.

For detailed information about creating object sharing rules, see the section Manage Object Sharing Rules for Access Groups in this chapter.

Step 3. Add Members to the Group

Finally, add resources to your new custom access group. You can add users to the group in a number of ways: manually add users on the UI, create group membership rules to automatically add users, or use the standard import and export functionality to add users.

Here are the steps to create group membership rules to add users to your group.

2. Click **Create Rule**.
3. On the Create Group Membership Rule page, enter a **Name** for the rule, for example, **Sales_Support_Resources** and optionally enter a rule **Description**.
4. Select the rule conditions. The conditions determine which resources are added or removed as members of the group.
   For example, you might specify that all resources that have an **Organization** attribute equal to **Sales Support** are added to the group.
5. Select **Save and Publish** from the **Actions** menu to publish the rule, then click **Save and Close** from the **Actions** menu.
6. On the Edit Access Group: Overview page, click **Save and Close** to save the group details.
   On the Access Groups page, check that your new group is included in the list of groups.
7. Now run the Run Access Group Membership Rules scheduled process to ensure that the access group membership rules are assigned and resources are added to the group.
   For information on running this process, see the topic Run the Access Group Membership Rules Process in this chapter.
Once the rules you created for your new access group are processed, all the users in the Sales Support organization will have access to all open opportunities.

For more detailed information about the different methods of adding users to custom access groups see the section Add Members to Custom Access Groups in this chapter.

For an example of how to assign access to sales objects to groups of users on the basis of the users home country, see the topic Assign Group Access By Country.

Edit Access Groups

After you create a custom access group, you can edit the group details. For example, you might want to activate a group, add new object sharing rules for the group, or add or remove group members. You can also edit system access groups to configure the rules assigned to the group.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Select the access group whose details you want to edit from the groups listed.

Custom access groups are displayed by default so if you want to edit a system access group, you first have to select **System Groups - Role** from the **List** drop-down menu. You can also choose to list all access groups or just active groups.

Details relating to the group and its members are listed on the Edit Access Group: Overview subtab.
3. What you can do depends on whether you’re editing a custom or a system group.
   - **System Groups**
     
     For system groups, you can review the group details and members on the Overview subtab but you can’t change any of this information and you can’t delete the group. System groups are predefined by Oracle and are automatically created and updated to reflect the job roles and user-job role assignments in your environment.
   - **Custom Groups**

     You can perform these actions from the Overview page for custom groups:

     - Change the group name or description.
     - Activate or inactivate a group.

     If you inactivate a group, group members lose any data access provided by the group.
     - Add group members by clicking **Add Members**.
     - Remove all group members who were added to the group manually by clicking **Remove Members**, or delete individual members from the group by clicking the **Remove** icon in the member row. Members who were added through group membership rules can’t be removed.
     - Delete the group by selecting **Delete Group** from the **Actions** menu.

     For information about deleting groups, see the topic Delete Access Groups.

4. Click the Object Sharing Rules subtab to view any predefined or custom object sharing rules defined for the group.
You can make these changes for both system and custom access groups:

- Enable or disable a predefined or custom rule for the access group by selecting or deselecting the **Enable** check box.
- Remove a custom rule or a predefined rule you added to the access group. Click the rule and on the Edit Object Sharing Rule page, select **Delete** from the **Actions** menu.

The rule is deleted for the group you're editing, but not for any other groups that the rule is associated with.

- Add a preexisting rule to the access group. Click **Add Rule**, and then search for and select the rule you want to add in the search dialog box.
- Create a new rule for the access group. Click **Create Rule**, and then define the new rule in the Create Object Sharing Rule page.
- Change the access level provided by the rule for this group by selecting a new value from the rule's **Access Level** drop-down list.

**Note:** If you're editing a system access group, a **Lock** icon is displayed for any predefined rules that are associated with the group as part of the default security configuration. For these rules, you can't change the access level for the group and you can't remove the rule from the group. The only change you can make is to enable or disable the rule for the group.

For information on object sharing rules, see the topic **Create Custom Object Sharing Rules**.

5. Click the Group Membership Rules subtab to view any group membership rules defined for the access group.

**Note:** You can't add members to system groups using group membership rules so this subtab isn't available for system groups.

You can edit an existing rule from this subtab by clicking the rule name link, or you can create a new rule by clicking **Create Rule**.

If you select an existing rule to edit, the Access Group: Edit Group Membership Rule page is displayed where you can edit or delete any of the rule details. For information on group membership rules, see the topic **Create Membership Rules for Custom Access Groups** in this chapter.

6. When you have finished editing the group details, click **Save and Close**.

Changes you make to object sharing rules or group membership rules are processed when the Object Sharing Rule Assignment Process or the Access Group Membership Rules Process is next run.

### Delete a Custom Access Group

You can delete a custom access group if you have the Delete Access Group privilege. By default, users assigned the IT Security Manager job role have this privilege. Sales Administrators aren't provided with the Delete Access Group privilege.

**Caution:** Once you delete a group and its members, you can't reactivate it. The users who were assigned to the group still exist but are no longer associated with the group and group members lose any data access provided by the group.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Select the access group you want to delete from the groups listed.
On the Edit Access Group: Group_Name page, select Delete Group from the Actions menu.
3. In the confirmation dialog, click Yes to confirm your choice.

The group is deleted and is no longer available on the Access Groups page.

Add Members to Custom Access Groups

Options for Assigning Members to Custom Access Groups

You can assign users to a custom access group when you create the group or you can add members at a later time. You can't assign users to system access groups. You can add members to a custom access group in any of these ways:

- Manually add members to a group on the Edit Access Group: Overview page. This option is useful if you only need to add a few users to a group on an ad-hoc basis.
- Create access group membership rules. Users who meet the conditions specified in the rule are automatically added to a group. Using group membership rules, you can add a large number of users to a group at once and simplify the process of maintaining the group's membership in the future. Users are added or removed from the group automatically depending on whether or not they meet the rule conditions.
- Assign users to groups using the standard import and export functionality. If you have large numbers of users to assign to one or more access groups on a one-off basis, you can import users and groups.

You can assign a user to one or more access groups and the user will have the data access permissions assigned to each group.

**Note:** You can only assign users who are assigned the Resource abstract role (ORA_HZ_Resource_Abstract) to groups.

Member Types

Access group members are categorized into member types according to how they're added to an access group:

- Manual members
  
  Users who are added to the group manually, either through the UI or through file import

- Rule members

  Users who are added to the group through rule processing

You can delete access group members on the Edit Access Group: Overview page if they were added to the group manually. Group members added through rule processing can't be manually removed from a group; they're only removed from a group if they no longer meet the rule conditions.

If a user is added to an access group more than once, manually and through group membership rule processing, the user is listed twice on the Edit Access Group: Overview page. You can delete the manual entry for the user but the user remains a group member provided they still satisfy the access group membership rule conditions.

For information about creating access group membership rules, see Create Access Group Membership Rules. For information about importing access groups and members, see the section Import and Export Access Groups and Members later in this chapter.
Add Members to Custom Access Groups Using the UI

You can manually add resource users to a custom access group at any time using the UI by performing these steps.

1. Navigate to the Access Groups page:
   - Sales Administrator: Navigator > Tools > Sales and Service Access Management
   - IT Security Manager: Navigator > Tools > Sales and Service Access Management > Configure Groups
2. On the Access Groups page, select the group you want to add members to.
   The Add: Group Members page is displayed.
4. Search for the member you want to add using one of the search fields.
   For example, in the First Name field, enter the first 3 characters of a user's first name and click Search. Or in the Role field, select a resource role to view all users assigned that role.
   If you create a custom field for the Resource object, for example, Country, you can use Application Composer to expose the field so that it's available as a drop-down list on the Add: Group Members UI. You can then search for resources using this field. In this example, you can search for users by country.
5. Select each of the users you want to add to the group in the Search Results area, then click Apply.
   Note: You can only assign users who are assigned the Resource abstract role (ORA_HZ_RESOURCE_ABSTRACT) to groups.
6. Search for and select any additional members you want to add to the group and, when you're finished adding members, click OK.
7. Verify that all the members you added to the group are listed in the Group Members area of the Edit Access Group: Overview page.
8. If you want to remove a member, click the Remove icon in the member row. To remove all members of the group who were added manually, click Remove All Members.
9. Click Save and Close to save the group membership details.

Create Membership Rules for Custom Access Groups

You can add resource users to a custom access group by defining one or more group membership rules. Each rule consists of conditions that determine which resources are added as members of the group. Any users who satisfy the conditions are automatically added to the access group and group members who no longer meet the conditions are automatically removed from the group. You can't remove members added through group membership rule processing using the UI.

Assigning members to groups using rules involves two steps: first you create and publish the membership rules, then you run the Access Group Membership Rules scheduled process to assign the rules.

Create Membership Rules
Here's how you can create a group membership rule to add members to your access group.

1. On the Access Group page, select the group you're creating the membership rule for.
2. On the Edit Access Group: Overview page, select the Group Membership Rules tab, then click Create Rule.
3. On the Access Group: Create Group Membership Rule page, enter a **Name** for the group membership rule and a **Description** if required.

4. In the Conditions section, specify the rule conditions.

   Each rule consists of one or more conditions that are evaluated individually. You can choose whether the rule action applies if any conditions are met, or only if all conditions are met, by choosing the appropriate value from the **Rule Applies If** list.

5. Enter a rule condition by clicking the **Add** icon, then enter these values for the condition.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Select either the <strong>Resources</strong> object or the <strong>Resources Hierarchy</strong> object. Only resource users can be added to an access group so you can only select one of these objects.</td>
</tr>
</tbody>
</table>
| Attribute  | Select an attribute from the list. Both custom and standard attributes defined for the object you selected are listed. **Note:** Support for a number of resource object attributes will be discontinued in future releases. So to prevent issues in the future:  
  - Avoid using these attributes: User Account Status, Company, Phone, Job Title, Manager First Name, Manager Last Name, Organizations, Teams, Usages  
  - Use custom attributes that are based on database columns only. Avoid using custom attributes, such as attributes based on the **Formula** field, that aren’t based on database columns. Support for attributes that aren’t based on database columns will be deprecated in future releases. |
| Operator   | Select the operator for your condition. For example, **Equals** or **Is blank**. **Tip:** If an attribute can have multiple values, such as the Roles or Teams attributes, use the **Contains** operator instead of the **Equals** operator to make sure that the condition adds all the intended resources to the group. For example, if you create a rule **Roles Equals Salesperson**, then users who are assigned only the Salesperson role are added to the group. If you create a rule **Roles Contains Salesperson**, then users assigned the Salesperson role and any other role are also added to the group. |
| Value      | Enter a value for the attribute, if relevant. If you’re entering more than one value, separate each value with a comma.                                                                                                                                                                                                                           |

Enter as many conditions as needed to suit your specific requirements. For example, if you want to add all resources who are sales representatives based in the Sales Support organization to your group, create two conditions with values similar to these and choose the **All conditions met** value from the **Rule Applies If** drop-down list.
Run the Access Group Membership Rules Process

Start the Run Access Group Membership Rules scheduled process to ensure that the access group membership rules are assigned. Once this process has run, all resources who meet the condition criteria are added to the access group. Here are the steps to run the scheduled process.

**Note:** Don't schedule or start the Run Access Group Membership Rules process at the same time as the Reporting Hierarchy Generation scheduled process. The Reporting Hierarchy Generation process updates the reporting hierarchy in accordance with changes to the internal resource or partner organization hierarchies and impacts the assignment of access group membership rules if both processes run at the same time.

1. In the **Navigator**, click **Tools > Scheduled Processes**.
2. On the **Overview** page, click **Schedule New Process**.
3. In the **Schedule New Process** window, enter **Run Access Group Membership Rules** in the **Name** field.
4. Select the process and click **OK**.
5. On the Process Details page, select the job parameters in the Basic Options region, then click **Submit** to run the process immediately. You can monitor its progress by searching for the **Run Access Group Membership Rules** process by name on the Overview page.

If you want to schedule the process to run at regular intervals, click **Advanced** on the Process Details page, then select the Schedule subtab in the Advanced Options region and enter your scheduling details. You can then click **Submit** to run the job according to your schedule.

**Tip:** It’s best practice to schedule the process to run every 24 hours for all records updated in the previous 24 hours. But if you edit the rule, it's also a good idea to run the process manually straight away.

6. When the process completes, navigate to the Edit Access Group: Overview page where you can see that all the resources who meet the rule conditions are added to the group. Notice that the **Member Type** field is set to **Rule** for all the new members.

When the Run Access Group Membership Rules process is next run, members are added to or removed from the group according to whether or not they satisfy the rule conditions.

You can edit a group membership rule at any time by selecting the rule from the Edit Access Group: Group Membership Rules page. You can also delete or inactivate the rule. If you delete or inactivate a rule, any users added to the group through the rule are removed when the Run Access Group Membership Rules scheduled process is next run.
Manage System Access Groups

Overview of System Access Groups

You can use system access groups and predefined rules to support team-, territory-, and management hierarchy-based access to data for your users. You can also provide users with global access to object data, or with fine-grained access to data such as Personally Identifiable Information (PII) for the Contact object. System access groups provide an alternative way to manage user access to data for supported objects. There’s a system access group to correspond to each of the standard sales and service job roles Oracle provides, and predefined object sharing rules assigned to each group provide the same access to supported object data as is provided by the standard job roles.

There are two types of system groups:

- Groups generated for each of the predefined sales and service job roles in your environment and for the Resource abstract role
- Groups generated for each of the custom job roles in your environment

On the UI, you can distinguish between the two types of system access groups as follows:

- The number assigned to system access groups generated for the predefined job roles and the Resource abstract role start with the ORA_ prefix. Access groups generated for your custom job roles don’t include the ORA_ prefix.
- The Predefined check box is checked for system access groups generated for the predefined job roles and the Resource abstract role but not for groups generated for your custom job roles.

Any user you assign to a predefined or custom job role is automatically included as a member of the associated system access group.

On the Access Groups main page, you can select the Update System Groups and Members option from the Actions menu. This option runs the Refresh Access Control Data Process so that system groups are updated with changes to the custom job roles and user-job role assignments in your environment.

What Changes Can You Make to System Groups?

You can't create new system groups or delete existing system groups. You also can't add or delete members of system groups, either manually, through group membership rules, or through import and export functionality. Users are automatically added to, or removed from system access groups according to the job roles they're assigned. You can add additional predefined or custom object sharing rules to system groups.

System Groups and Predefined Rules

Each system group for a predefined job role is associated with predefined object sharing rules that provide group members with the same access to data for supported objects that the relevant job role provides through its predefined data security policies. The association between system groups and predefined rules is part of the default security
configuration and can't be changed, but this association is disabled by default. Each predefined rule is also inactive by default. So to use system groups to manage user access to data, you must first:

- Activate each of the predefined rules you want to use
- Enable the association between the group and the predefined rules

**Note:** System groups created for custom job roles aren't associated with any object sharing rules. You add the rules you want to assign to the group manually.

**Objects Supported for Predefined Rules**

Predefined rules aren't currently available for all sales objects. You can now use predefined rules to provide access to data for these objects:

- Account
- Campaign
- Contact
- Opportunity
- Sales Lead

**Enable the Predefined Rules for a System Access Group**

If you want to use system access groups provided by Oracle to manage your user's access to supported object data, you must enable the predefined rules for each system access group using these steps.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. From the **List** drop-down list, select **System Groups - Role** to display all system access groups.
3. Click the name of a system access group whose rules you want to enable.

Details relating to the group and its members are listed on the Edit Access Group page.
4. Click the Object Sharing Rules subtab to view the object sharing rules defined for the access group.

On the Object Sharing Rules UI, all the custom and predefined rules assigned to the group are listed.

- The predefined rules associated with the access group as part of the default security configuration have a **Lock** icon and the **Predefined** check box is selected. You can't change any of the rule details, including the access level specified in the rule.
- If you added a predefined rule to the group yourself, the **Predefined** check box is selected but the rule doesn't have a **Lock** icon. You can change the access level of the rule for the group.

5. To enable each of the rules associated with this system group as part of the default security configuration, select the **Enable** check box for each rule.
6. Click **Save** to save your changes.
7. To activate each of the predefined rules you enabled:
   a. Click the rule name link in the **Name** field.
   b. On the Edit Object Sharing Rule page, click the **Active** check box.
   c. From the Actions menu, click **Save and Publish**.
**Note:** Users must be assigned the Grant on Application Objects data security policy to publish individual rules that provide global access to object data. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege. If you use custom versions of these roles, assign this privilege to your custom roles.

d. Click **Save and Close**.

8. On the Edit Access Group page, click **Save and Close**.
9. Run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the access group sharing rules for each object are assigned properly.

For information, see the topic Run the Perform Object Sharing Rule Assignment Process in this chapter.

### Run the Refresh Access Control Data Process for System Groups

On the Access Groups main page, you can select the **Update System Groups and Members** option from the Actions menu to run the Refresh Access Control Data scheduled process. Running this process ensures that system groups shown on the UI reflect changes to the custom job roles and user-job role assignments in your environment. You also need to schedule this process to run periodically in accordance with your business requirements. These are the steps to schedule the process.

1. In the Navigator, click **Tools > Scheduled Processes**.
2. On the Overview page, click **Schedule New Process**.
3. In the Schedule New Process window, enter **Refresh Access Control Data** in the **Name** field and press **Enter**.
4. Select the process and click **OK**.
5. On the Process Details page, select whether you want to perform a full or an incremental refresh of the data by selecting the appropriate option from the **Refresh Type** drop-down list in the Basic Options area.
6. To schedule the process to run regularly use these steps.

   How frequently you run the process will vary according to your business requirements but, in general, it's a good idea to run the process daily.

   a. Click **Advanced** on the Process Details page.
   b. Click the Schedule tab in the Advanced Options area and select the **Using a schedule** option.
   c. Select how often you want the process to run from the **Frequency** drop-down list.

   For example, select **Daily**.
   d. Indicate when you want the schedule to start and end by entering values in the **Start Date** and **End Date** fields.
   e. Click **Submit**.

   Depending on your settings, your process runs immediately or at the intervals you specified. You can monitor its progress on the Overview page.

### Manage Object Sharing Rules for Access Groups
Overview of Object Sharing Rules

Object sharing rules provide access groups with access to an object’s records. There are two types of object sharing rules:

- Custom rules you create to configure data access for members of access groups.
  You must manually assign these rules to relevant access groups and the rules are active by default.
- Predefined rules created by Oracle.
  One or more predefined rules are assigned to each system access group that’s generated for a predefined job role. These rules provide the same access to data for supported objects as the job role provides. The association between a system group and the predefined rules assigned to it isn't enabled by default and each predefined rule is also inactive by default.

On the Object Sharing Rules page, the **Predefined** column is checked if a rule is predefined. If the predefined rule is assigned to a system access group as part of the default security configuration, it also has a Lock icon to indicate that you can’t change the association between the rule and the group, or the level of access provided by the rule to the group.

Both types of object sharing rules specify the object the rule is created for, the condition that must be met for the rule to be applied, the access group the rule is assigned to and the access level that group members receive. You can also create an access extension rule for both custom and predefined rules, and can activate or inactivate both types of rules.

But there are also a few differences between the object sharing rules you create and the predefined rules Oracle provides. There are also differences in what you can do when a predefined rule is associated with a system group as part of the default security configuration and when it isn’t.

Comparison of the Predefined and Custom Object Sharing Rules

Some of the similarities and differences between the object sharing rules you create and the predefined rules are outlined in the table.

<table>
<thead>
<tr>
<th><strong>Custom Rules</strong></th>
<th><strong>Predefined Rules</strong></th>
<th><strong>Predefined Rules Associated to a System Group</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can create, edit, and delete the rule.</td>
<td>Oracle creates the rule. You can edit the rule.</td>
<td>You can only enable or disable the rule for the group.</td>
</tr>
<tr>
<td>Rule is active by default.</td>
<td>Rule is inactive by default.</td>
<td>Rule is inactive by default.</td>
</tr>
<tr>
<td>You can create one or more conditions for the rule.</td>
<td>Rule has one predefined condition which you can’t change.</td>
<td>Rule has one predefined condition which you can’t change.</td>
</tr>
<tr>
<td>You can’t create rule conditions that provide either of these types of access:</td>
<td>Predefined rules with conditions that provide global and field-level access to object data are provided.</td>
<td>Predefined rules with conditions that provide global and field-level access to object data are available.</td>
</tr>
</tbody>
</table>
  - Access to all of an object’s records
  - Field-level access to object records, such as access to Personally
<table>
<thead>
<tr>
<th>Custom Rules</th>
<th>Predefined Rules</th>
<th>Predefined Rules Associated to a System Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifiable Information (PII) for the Contact object</td>
<td>You can assign the rule to system access groups and custom access groups.</td>
<td>NA</td>
</tr>
<tr>
<td>You can assign the rule to system access groups and custom access groups.</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>Note: Predefined rules that provide global or field-level access to object data are an exception. You can't assign these rules to custom access groups.</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>You can change the access level provided by the rule for different custom or system groups.</td>
<td>You can change the access level provided by the rule for a custom access group. If a rule is predefined but doesn't have the Lock icon, you can also change the access level provided by the rule to a system group.</td>
<td>Can't change the access level provided by a predefined rule for a system access group.</td>
</tr>
</tbody>
</table>

Create Custom Object Sharing Rules

Once you have created an access group you can create rules to provide the group with access to an object's records. You can define rules for both standard and custom objects.

To create a custom object sharing rule, you specify the type of object access to be provided, the conditions under which the access is provided, and the groups to share the rule with. You then publish the rule to Assignment Manager. Finally, you run the Perform Object Sharing Rule Assignment Processing task to enable the resources in the associated access group to have access to the object data records.

This topic describes how to create object sharing rules from an object context. But you can also create a rule in the context of a group when editing the group. For additional information see the topic Edit Access Groups.

Here are the steps to create object sharing rules.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
   The Object Sharing Rules page is displayed. From here, you can modify an existing rule or create a new rule to share with an access group.
3. To make sure that any custom attributes or objects created in Application Composer that are enabled for access groups are available on this UI, select the Synchronize Custom Objects and Fields option from the Actions menu.
   For more information about using custom objects with access groups, see the topic Enable Access Group Security for Custom Objects.
4. Select the object you want to provide access to from the Object list. For example, select Opportunity.
   For a list of objects supported with access groups, see the topic Overview of Access Groups.
5. To create a new object sharing rule, click Create in the Rules section.
The Rules section lists any object sharing rules you previously created for this object and any predefined rules for the object.

6. On the Create Rule page, enter a Name and Description for the new rule.

7. New rules are set to Active by default. Deselect the Active check box if you don't want to activate the rule just yet.

8. In the Conditions section, specify the rule conditions.

9. You can optionally select a predefined condition to use with the custom conditions you're about to create from the Predefined Condition list.

**Note:** The Predefined Condition list is only available if this functionality is enabled in your environment. For additional information on this functionality, see the topic Combine Predefined and Custom Conditions in a Rule.

10. Each condition in a rule is evaluated individually. You can choose whether the rule action applies if any custom conditions are met or only if all custom conditions are met by choosing the appropriate value from the Rule Applies If list.

11. Enter your first condition. For example, if you want to give group members read access to all opportunities associated with their home country, create a rule with values similar to these:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Opportunity</td>
</tr>
<tr>
<td>Attribute</td>
<td>Country (this is a custom field for the Opportunity object)</td>
</tr>
<tr>
<td>Operator</td>
<td>Equals</td>
</tr>
<tr>
<td>Value</td>
<td>UK</td>
</tr>
</tbody>
</table>

Here are some considerations to keep in mind when selecting the attributes to use in rule conditions.

- By default, not all of the standard attributes for an object are displayed on the Access Groups Create Rule or Edit Rule UIs. To make additional standard attributes available for an object, follow the steps in the topic Enable Additional Attributes for Access Group Object Sharing Rules.
- Support for the object attributes listed in this table will be discontinued in future releases. When creating conditions, it's a good idea to avoid using these attributes.

<table>
<thead>
<tr>
<th>Object</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Phone</td>
</tr>
<tr>
<td>Activity</td>
<td>Account, Asset, Business Plan, Campaign, MDF Claim, Deal Registration, Delegated By, MDF Request, Lead, Opportunity, Enrollment Number, Partner, Program, Sales Objective, Service Request</td>
</tr>
</tbody>
</table>
### Object | Attribute
--- | ---
Asset | Asset Owner, Product
Account | Type, Favorite, Organization Type
Opportunity | Business Unit, Win Probability (RcmndWinProb)
Deals | Account Country
Product | Eligible for Service

- Use custom attributes that are based on database columns only. Avoid using custom attributes, such as attributes based on the Formula field, that aren't based on database columns. Support for attributes that aren't based on database columns will be deprecated in future releases.

12. Enter any additional conditions required to specify the access level you want the rule to provide.
13. Next, in the Action: Assign Access Group section, click Select and Add from the Actions menu.
14. Search for and select the access group you want to share this rule with, then click Apply and then Done.

You can assign a rule to multiple access groups.
15. In the Access Level field, select the type of object access you want to give group members.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Access Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Read-only access</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you’re creating a rule for the Sales Quota Plan object, only the Read access level is supported.</td>
</tr>
<tr>
<td>Update</td>
<td>Read and update access</td>
</tr>
<tr>
<td>Delete</td>
<td>Read and delete access</td>
</tr>
<tr>
<td>Full</td>
<td>Read, update and delete access</td>
</tr>
</tbody>
</table>

16. Select Save and Close from the Actions menu.
17. On the Object Sharing Rules page, publish the new rule to ensure that your changes get included in the assignment processing by selecting Publish Rules from the Actions menu.
18. When the status indicator shows the publish process has completed, click Close.
19. Run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the access group sharing rules for each object are assigned properly. It’s a good idea to schedule this process to run frequently.
Tip: You might want to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object. See the topic Run the Perform Object Sharing Rule Assignment Process for more information.

Combine Predefined and Custom Conditions in a Rule

You can create hybrid object sharing rules for your access groups, that is, rules that combine a predefined condition with one or more custom conditions, by enabling the profile option System and Custom Rule Conditions Combination Supported. Once this profile option is enabled, a Predefined Condition list becomes available in the Conditions section of the Create Rule page where you can select a predefined condition. Combining custom conditions with a selected predefined condition in a hybrid rule lets you refine the access that’s provided by the predefined condition.

For example, there is a predefined condition that provides all users who are on the opportunity team with access to the opportunity. If you want to restrict this access so team members have access to the opportunity only if it has a status of Open, then you can do so using these steps.

1. Create an object sharing rule for the Opportunity object.
2. In the Conditions section, select this condition from the Predefined Condition list: Opportunities where the access group member is on the opportunity team.
3. Select a value from the Rule Applies If list to choose whether the custom conditions you’re about to create are applied when any of the custom conditions are met, or only when all the custom conditions are met. The default value is All Conditions Met.
4. Create a rule with values similar to these.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Opportunity</td>
</tr>
<tr>
<td>Attribute</td>
<td>Status</td>
</tr>
<tr>
<td>Operator</td>
<td>Equals</td>
</tr>
<tr>
<td>Value</td>
<td>Open</td>
</tr>
</tbody>
</table>

5. In the Action: Assign Access Group section, select the access group you want to share this rule with and the type of access to give group members.
6. Select Save and Close from the Actions menu to save the rule.

All users on an opportunity sales team can now view the opportunity provided it has a status of open.

Considerations When Using Predefined Conditions in a Rule

Here are some considerations to keep in mind when creating an object sharing rule that uses a predefined condition.

- You can select only one predefined condition for the rule.
• You have to define at least one custom condition for the rule.
• Once you have created and saved a rule containing a predefined condition, you can’t change the predefined condition selected for the rule.
• If you create rules containing a predefined condition, then disable the profile option that lets you use predefined conditions in a rule, this is what happens:
  o On the Create Rule page, the **Predefined Condition** list is no longer available.
  o When you edit an existing hybrid rule, the predefined condition is visible in the **Predefined Condition** field on the Edit Rule page but you can’t change the predefined condition.
  o If an existing hybrid rule is assigned to an access group, group members continue to receive the data access provided by the rule.

Enable the Profile Option

Use these steps to enable the profile option System and Custom Rule Conditions Combination Supported.

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search for the profile option code **ORA_MOW_SUPPORT_SEEDED_CONDITION**.
3. In the **Profile Values** section, select **Yes** from the **Profile Value** field.
4. Click **Save and Close**.

Edit Object Sharing Rules

You can edit the predefined or custom object sharing rules at any time. For example, you might want to assign a rule to additional access groups, or change the level of access a rule provides to a specific group. Depending on what you want to do, you can choose to edit the object sharing rules from either of these locations:

• The **Edit Access Group: Object Sharing Rules** subtab (group context)
  You can review and edit all the object sharing rules assigned to a specific access group, either by you or by Oracle, when editing an access group. Reviewing rule information from a group context is useful if you want to see what access group members have to data for different objects, or if you want to enable all the predefined rules assigned to a system group. For additional information, see the topic **Edit Access Groups** in this chapter.

• The **Object Sharing Rules** page (object context)
  You can review or edit all the predefined and custom object sharing rules and access extension rules that have been created for a specific object on the Object Sharing Rules page. If you want to delete a custom rule, or edit an access extension rule, you can only do so from this page.

Follow these steps to edit rules from an object context.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
3. On the Object Sharing Rules page, select the object you want to review from the **Object** list.
   All the rules and access extension rules defined for the object are listed.
4. Search for and select the rule whose details you want to edit.
   Details relating to the rule are displayed on the Edit Rule UI.
5. The changes you can make to a rule vary depending on whether you’re editing a predefined rule or a rule you created yourself. But to use either type of rule, the rule must be active. Rules you create are active by default, but predefined rules are inactive. To activate a rule, or inactive a rule you no longer require, select or deselect the **Active** check box.
6. If you're editing a custom object sharing rule you created, you can delete the rule by selecting Delete from the Actions menu.

Provided the rule isn't assigned to any access groups, the rule is deleted. You can't delete predefined rules.

7. Editing rule conditions:
   - If you're editing a predefined rule, you can't change the condition defined for the rule, delete the condition or add new conditions.
   - If you're editing a rule you created, you can create new conditions, or edit or delete the existing conditions in the Conditions area. For information on defining rule conditions, see the topic Create Custom Object Sharing Rules.

8. Editing access groups:

The access groups the rule is assigned to are listed in the Action: Assign Access Group area. You can make these changes for both predefined and custom object sharing rules:

   - Enable or disable the rule for a specific access group by selecting or deselecting the Enable check box.
   - Remove an access group from the list by selecting the group and then selecting the Delete option from the Actions menu.
   - Change the access level provided by the rule for a specific group by changing the value in the Access Level drop-down list.
   - Assign the rule to additional custom or system access groups by performing these steps:
     - Select the Select and Add option from the Actions menu.
     - In the Select and Add: Access Group dialog box, search for and then select the custom or system access group you want to assign the rule to, then click Apply.
     - Add any other groups and, when you have completed your selections, click Done.

Note: For a predefined rule for which Oracle has created the rule-system group association, a Lock icon indicates that this association is part of the default security configuration. In these cases, you can't edit the rule to change the access level for the group and you can't remove the rule from the group. The only change you can make is to enable or disable the rule for the group.

9. When you complete all your editing changes, click Save and Close from the Edit Rule page Actions menu.

10. On the Object Sharing Rules page, select the Publish Rules option from the Actions menu to apply the changes you made.

11. Run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the access group sharing rules for each object are assigned properly.

Overview of Access Extension Rules

Create access extension rules to extend the access defined for an object in an object sharing rule to a related object. For example, if you have secured access to an object such as Account using object sharing rules, you can extend the access defined for the Account object to a related object, such as Activity, by creating an access extension rule. All members of an access group who can access account data will then have access to activity data for the account with the access level you choose in the access extension rule.
Supported Objects
Access extension rules functionality isn't currently supported for all the objects that are enabled for access groups. You can create an access extension rule only for these objects.

- Activity
- Contact
- Custom objects
- Deal Registration
- Sales Lead
- MDF Budget
- MDF Claim
- MDF Request
- Opportunity
- Program Enrollments
- Sales Orders (Quotes and Orders)

You can define as many access extension rules as required for each object.

Considerations When Using Access Extension Rules
Before creating an access extension rule for an object, review the following considerations.

- You can't link access extension rules.

  Each access extension rule provides access to records for only one object and can't be extended to provide access to records for a second object.

  For example, if you create an access extension rule to provide group members with access to activity data for accounts they can access (Rule 1), you can't create another rule to grant access to opportunities on the basis of the activities they can access through Rule 1. In this scenario, you have to create two new access extension rules for the Opportunity object:

  - A rule to provide opportunity access based on the group members access to activities
  - A rule to provide opportunity access based on the group members access to accounts

- When you define a relationship between two objects in Application Composer, you can optionally specify data filter criteria for both the source and target objects. The filter criteria control which records are available for association at runtime with a record from the other object in the relationship.

  Access Extension rules don't support filters, so if you create an access extension rule for related objects with filters, be aware that the filter isn't applied. For additional information about object relationships, see the Configuring Applications Using Application Composer guide.

- You can't extend the access of rules that provide global access to an object's data to related objects.
Create Access Extension Rules

Create access extension rules to extend the access defined for an object in an object sharing rule to a related object using these steps.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, click the Object Sharing Rules tab.
3. Select the **Synchronize Custom Objects and Fields** option from the **Actions** menu to make sure that custom attributes or objects that are enabled for access groups are available on the UI.
4. Select the object you're creating the extension rule for in the **Object** drop-down list. For example, select the **Activity** object.

Any existing object sharing rules or access extension rules defined for the object are displayed.
5. In the Access Extension Rules area, click **Create**.
6. On the Create Access Extension Rule page, specify these values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the rule. It's a good idea to use a meaningful name that identifies the purpose of the rule. For example, if you're creating a rule to extend the access defined for an account to its related activities, you might name the rule something like ActivityToAccount.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter additional details about the rule if required.</td>
</tr>
<tr>
<td>Active</td>
<td>Rules are active by default. Deselect the <strong>Active</strong> check box if you're not yet ready to apply the rule.</td>
</tr>
</tbody>
</table>

7. From the **Related Object** list, select the object whose access you want to extend.

All the object sharing rules defined for the related object you selected are listed in the rules table.

**Note:** Only objects related to the object you're creating the rule for are listed in the **Related Object** list. For standard objects, the relationship between objects is predefined by Oracle. For example, if you're creating the rule for the Activity object, then the default related objects include Account, Contact, Sales Lead, Opportunity. But if you used Application Composer to define a custom relationship between two standard objects, between a custom object and a standard object, or between two custom objects, then additional objects are also available to select.

8. Select one of these options depending on what you want to do:

   - **Extend all access defined for related object**
     
     Select this option if you want to extend the access provided by all the rules to all the groups assigned the rule.

     Any access group members assigned access to the related object by any of the rules listed is assigned the same access to the object you're creating the extension rule for. You can't change the level of access provided by the rules.
Select rules to extend access defined for related object

Select this option if you want to extend the access of only the rules you select to only the groups you select.

When you select this option, the Read, Update and Delete access level check boxes for each rule in the rules table are deselected.

- To apply a rule to your selected object, click one or more of the check boxes for the rule. For example, click the Update check box for a rule to specify that anyone who can access the related object (for example, Account) can update data for the object you’re creating the rule for (for example, Activity).
- There’s a separate row for each rule-group combination so you can choose to extend the access provided by a rule only to a specific access group or to a number of groups.
- If you don’t want to apply a rule, leave the access level check boxes for the rule unchecked.

9. Click Clear at any time to deselect all the Read, Update, and Delete selections you made.

10. Click Save and Close to save your changes.

11. Publish the new rule on the Object Sharing Rules page by selecting the Publish Rules option from the Actions menu.

12. When the status indicator shows the publish process has completed, run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the access extension rule is assigned.

Related Topics
- Configuring Applications Using Application Composer

Run the Perform Object Sharing Rule Assignment Process

Run the Perform Object Sharing Rule Assignment process to assign access group object sharing rules to objects each time you add an access group and share rules. You must also run this process periodically in accordance with your business requirements to make sure you have the required access to all records and object data for your selected access groups. If you require immediate access to new records and objects, you can manually submit the Perform Object Sharing Rule Assignment process to run immediately.

For example, a rule already exists for the account object and you create a new account record. You won’t have real time access to this record based on the existing object rule until the next scheduled run of the Perform Object Sharing Rule Assignment job. If you want to access the new account record immediately, you can submit the job on an ad-hoc basis.

You can also run the Object Sharing Assignment Job Set to assign a batch of access group object sharing rules for all the available assignment objects. A job set contains multiple jobs. The job is the executable that controls what the process can do and what parameters and other options are available to you to run the process. You can schedule these jobs to run regularly to ensure that all access group object sharing rules, records, and object data for your selected access groups are assigned and available to you.

Perform Object Sharing Rule Assignment Processing

Here’s how to run the Perform Object Sharing Rule Assignment job for the account object:

1. In the Navigator, click Tools > Scheduled Processes.
3. In the Schedule New Process window, enter Perform Object Sharing Rule Assignment Processing in the Name field and press Return.
4. Select the process and click OK.
Here's a screenshot of the Process Details page.

5. On the Process Details page, enter these details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Object</td>
<td>Select the work object you want from the drop-down list.</td>
</tr>
<tr>
<td>Record Selection</td>
<td>You can run the assignment process on a subset of records. Select from the following list:</td>
</tr>
<tr>
<td></td>
<td>o All records</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>You might want to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object.</td>
</tr>
<tr>
<td></td>
<td>Enter a record selection value for these options:</td>
</tr>
<tr>
<td></td>
<td>o Records updated in last ’X’ days</td>
</tr>
<tr>
<td></td>
<td>o Records updated in last ’X’ hours</td>
</tr>
<tr>
<td></td>
<td>o Records updated between dates</td>
</tr>
<tr>
<td></td>
<td>o Single record</td>
</tr>
<tr>
<td>Maximum Sub Processes per Process</td>
<td>If the number objects created is less than 500 thousand, then leave the default option of 2 as the maximum number of sub processes per process. The following recommendation is only applicable for when this process is run for the first time or for a complete run for all objects. However, the next time you run the process, only the changed objects are processed. If</td>
</tr>
</tbody>
</table>
you're executing incremental runs at periodic scheduled times, then there's no need to update the default value of 2.

Oracle recommends changing this value if the number of objects is:

- Between 500 thousand and 1 million objects enter 5
- Greater than 1 million objects, enter 10
- Greater than 5 million objects, enter 20
- Greater than 10 million objects, enter 30

6. The first time you run the process click **Submit** to run it immediately.

Depending on your settings, your process runs immediately or at the intervals you specified. You can monitor its progress by searching for the Perform Object Sharing Rule Assignment Processing process by name on the Overview page.

You can also schedule the process to run regularly using the following steps. How frequently you run the process will vary according to your business requirements but, in general, it’s a good idea to run the process hourly.

1. Click **Advanced**.
2. Click the Schedule tab.
3. Select the **Using a schedule** option.
4. Select the frequency and start date.
5. Enter an end date far in the future.
6. Click **Submit**.

### Run the Object Sharing Assignment Job Set

Here’s an example of the steps to run the Object Sharing Assignment Job Set for your access groups.

1. Navigate to the **Setup and Maintenance** area, and search for the **Manage Enterprise Scheduler Job Definitions and Job Sets for Customer Relationship Management and Related Applications** task.
2. Click the **Manage Job Sets** tab and create a job set with the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required)</td>
</tr>
<tr>
<td></td>
<td>For example: ObjectSharingAssignmentEssJobSet</td>
</tr>
<tr>
<td>Display Name</td>
<td>(Required)</td>
</tr>
<tr>
<td></td>
<td>For example: Object Sharing Assignment ESS Job Set</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional)</td>
</tr>
</tbody>
</table>
### Access Groups

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>(Optional)</td>
</tr>
<tr>
<td></td>
<td>Enter the custom path</td>
</tr>
</tbody>
</table>

3. In the **Job Set Steps** section, select **Parallel** and click the plus (+) icon to display the **Edit Step** window.
4. Enter 1 or any unique number in the Step ID field.
5. Enter ObjectShareBatchAssignRequest in the **Job** field and click **OK**.
6. Repeat Step 4, 5 and 6 based on the number of jobs you want to trigger in parallel. For example, if you want to run Perform Object Sharing Assignment in parallel for two objects, Account and Opportunity, then, create two Job Set Steps.
7. Next, click the **System Properties** tab from the **Edit Step** window.
8. Click the plus (+) icon to display the **Add System Property** window and enter the following:
   - **Name**: SYS_effectiveApplication
   - **Type**: String
   - **Initial Value**: CrmEss
9. Click **OK**.
10. Click **Save and Close**, and then **Done**.

Now the newly created Job Set is listed in the Scheduled Process UI.

11. In the Navigator, click **Tools > Scheduled Processes**.
12. On the Overview page, click **Schedule New Process**.
13. In the Schedule New Process window, select **Job Set** and search and select the newly created Job Set by display name.
14. Click each newly created job set and add the parameters accordingly.
15. The first time you run the job set process, click **Submit** to run it immediately.

Depending on your settings, your process runs immediately or at the intervals you specified. You can monitor its progress by searching for the job set process by name on the Overview page.

You can also set up the process to run regularly per your business requirements.

**Related Topics**

- **Schedule Account Assignment**

### Enable Additional Attributes for Access Group Object Sharing Rules

Use the Manage Object Sharing Assignment Objects task to add additional attributes and make them available for your selected rules when you create or edit a standard object sharing rule. You create object sharing rules to associate with access groups and if the attribute value that you want isn't available from the rule conditions drop-down list, you can enable the attributes you want from here.
Once you set up the rules with the conditions that records must meet, then resources from your access groups get assigned to the object when they match the rule conditions.

**Note:** This procedure isn’t needed for any custom objects. It’s needed only if you want to expose additional attributes for one of your standard objects. Custom objects and attributes created in Application Composer are synchronized and available when you select the **Synchronize Custom Objects and Fields** menu item from the **Actions** menu on the Object Sharing Rules page.

Here’s an example of the steps to enable an Opportunity object rule attribute for your access group.

1. Navigate to the **Setup and Maintenance** area, and search for the **Manage Object Sharing Assignment Objects** task.
2. On the Manage Object Sharing Assignment Objects page, select the **Opportunity** work object.
3. In the **Opportunity: Details** section, select the **Attributes** tab.
   - The attributes defined for the selected Opportunity object are displayed.
4. Click the attribute that you want to add to an Opportunity record rule that you want to share.
   - For example, if you want to provide the access group called High_Tech_Oppti_Members with access to the all opportunities for the GreenServer account based on the Asset ID, then enable the attribute **Asset ID** to include in your combination of attributes for the sharing rule.
5. Click **Save and Close**.

Once the additional attributes are enabled, setup the rules using the Object Sharing Rules page. See the topic **Manage Object Sharing Rules for Access Groups** for more information.

Run the **Perform Object Sharing Rule Assignment Processing** scheduled process to ensure that the access group sharing rules are assigned properly. See the topic **Run the Perform Object Sharing Rule Assignment Process** for more information.

### Enable Access Group Security for Custom Objects

You can use access groups to provide resources with access to custom object data. To do this, you must first enable access group security for each custom object.

To enable access group security for custom objects, complete these steps:

1. Navigate to Application Composer and confirm that you're in an active sandbox.
2. Navigate to the Security node of the custom object that you want to enable access group security for.
4. Next, enable that custom object for access group object sharing rules. To do this, navigate to the Access Groups page in the Sales and Service Access Management work area.
5. On the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** item from the **Actions** menu. The custom object and its attributes are now available when defining object sharing rules for access groups.
   - Navigate to the custom object’s Security node, and configure functional security in the Roles section of the Define Policies page. This step isn’t related to access group security (data security), but it’s a required step so that the right roles can see the custom object’s user interface pages (functional security).

After you enable access group security for a custom object, you work with it just like a standard object. Create your object sharing rules for access groups, and all group members are given access to that custom object’s data according to the rules.
Tip: When configuring data security, you can optionally configure owner security instead of access group security. With owner security, for example, you can provide create and read access to all users, update access to the record’s owner and owner management chain, and delete access to only the owner. You configure owner security in the Roles section of the Define Policies page. If you configure both owner and access group security, then your users will see data from both their owner management chain as well as from access groups that they’re members of.

Disabling Access Group Security for a Custom Object

You can disable access group security for a custom object, too.

1. In the Sales and Service Access Management work area, inactivate the object sharing rules for the custom object.
2. Run the Perform Object Sharing Rule Assignment Processing process for the custom object.
3. Cancel all future object sharing scheduled processes for the object.
4. Next, go to Application Composer:
   a. Navigate back to the object’s Security node in an active sandbox.
   b. Confirm that the Enable Access Group Security check box isn't selected and that its data security policy is configured properly for each role.
   c. Publish the sandbox.
5. Finally, back in the Sales and Service Access Management work area, select the Synchronize Custom Objects and Fields item from the Actions menu on the Object Sharing Rules page. This hides the custom object and its rules.

Assign Group Access By Country

If you want to provide a group of users with access to data on the basis of the user’s context, such as their business unit, country or region, then access groups are the best way of doing this.

This topic gives an example of the high-level steps to follow to assign access to sales objects (Accounts, Contacts, Opportunities, Partners and Leads) to groups of resource users on the basis of the users home country. You can use a similar process to assign a group with data access using some other attribute, such as resource organization.

These are the steps to provide users with access to sales records on the basis of the user’s country.

1. Create a custom attribute, Country, for each sales object and make the attribute available as a custom field on the sales object UI.
   
   When creating or editing an object record, such as an opportunity, the user can then select the country associated with the record from the custom Country field on the UI.

2. Create a custom attribute, Country, for the Resource object to represent a user’s country and make the attribute available as a custom field on the Resource object UI.
   
   When creating users, you can then select the country the user is associated with from the Country field on the UI.

3. On the Access Groups page of the Sales and Service Access Management work area, create an access group for each country and add existing resources to each country group. As new users join your organization, make sure you add them to a country group.
You can add members to each country-based access group manually on the Access Groups UI. Or use these steps to add members to access groups using the export and import functionality:

a. Use the resource export functionality to generate a list of sales resources and filter the generated export file based on the **Country** field.
b. Import country groups and members:
   - Create an import file similar to the following for each country-based access group.

<table>
<thead>
<tr>
<th>ACCESS_GROUP_NUMBER</th>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>ACTIVE_FLAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>3788493471</td>
<td>GERMAN REGION</td>
<td>Access group for users in Germany</td>
<td>Y</td>
</tr>
<tr>
<td>3788493472</td>
<td>UK</td>
<td>Access group for users in UK</td>
<td>Y</td>
</tr>
<tr>
<td>3788493473</td>
<td>FRANCE</td>
<td>Access group for users in France</td>
<td>Y</td>
</tr>
</tbody>
</table>

   - Create an import file of resources similar to the following to add members to each access group.

<table>
<thead>
<tr>
<th>ACCESS_GROUP_NUMBER</th>
<th>GROUP_NAME</th>
<th>PARTY_NUMBER</th>
<th>RESOURCE_EMAIL_ADDRESS</th>
<th>PARTY_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>3788493471</td>
<td>GERMAN REGION</td>
<td>2793920203</td>
<td><a href="mailto:tom.jones@example.com">tom.jones@example.com</a></td>
<td>Tom Jones</td>
</tr>
<tr>
<td>3788493471</td>
<td>GERMAN REGION</td>
<td>2793920204</td>
<td><a href="mailto:lisa.jones@example.com">lisa.jones@example.com</a></td>
<td>Lisa Jones</td>
</tr>
<tr>
<td>3788493471</td>
<td>GERMAN REGION</td>
<td>2793920205</td>
<td><a href="mailto:matt.hooper@example.com">matt.hooper@example.com</a></td>
<td>Matt Hooper</td>
</tr>
<tr>
<td>3788493471</td>
<td>GERMAN REGION</td>
<td>2793920206</td>
<td><a href="mailto:jane.smith@example.com">jane.smith@example.com</a></td>
<td>Jane Smith</td>
</tr>
</tbody>
</table>

4. On the Access Groups page, click the **Object Sharing Rules** tab.
5. To make the Country attribute visible and available for selection on the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** item from the **Actions** menu.
6. When the value of the **Last Synchronized** field indicates that the synchronize process is finished, select the sales object that you want to assign by country, for example, **Opportunity**.
7. Create an individual rule for each country by clicking **Create** in the Custom Rules region.
   a. In the Conditions region of the Create Rule page, in the **Attribute** field, select the **Country** attribute as the value used to assign object records.
   b. In the Action: Assign Access Group region, assign the rule to the relevant country-based access group and select the level of object access to be provided. For example, select **Read** or **Update** access.
   c. Click **Save and Close** from the **Actions** menu to save the rule.
The Object Sharing Rules page is displayed.

8. When you have created an object sharing rule for each country, on the Object Sharing Rules page select **Publish Rules** from the **Actions** menu to publish all new and changed rules for the object.

9. Run the Perform Object Sharing Rule Assignment Processing process so that the access group sharing rules for the object are assigned properly.

   It's a good idea to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object.

For additional information about creating custom attributes and making them visible on a UI, see the Configuring Applications Using Application Composer guide. For additional information about importing and exporting data, see the guide Understanding Import and Export Management for CX Sales and B2B Service.

Related Topics
- [Oracle CX Understanding Import and Export Management for CX Sales and B2B Service](#)
- [Oracle Applications Cloud Configuring Applications Using Application Composer](#)

### Import and Export Access Groups, Members, and Rules

#### Overview

You can use the standard export and import framework to export and import access groups objects.

- **You can import and export access groups and access group members.**
  
  For example, if there are thousands of sales representatives in your organization and you want to assign them to an access group, you could search for all users who are assigned the Sales Representative role and export this list of users to a CSV file. You could then edit the file to specify the name of the access group the users are to be assigned to, then import the updated CSV file.

- **You can also export access group rules, including group membership rules and object sharing rules, to a CSV file.**
  
  You can then use the file to review and analyze all the rules in your environment.

  You can't import access group rules; you must create these individually in the Object Sharing Rules UI or the Group Membership Rules UI.

For additional information about importing and exporting data, see the guide Understanding Import and Export Management for CX Sales and B2B Service on Oracle Help Center.

Related Topics
- [Oracle CX Understanding Import and Export Management for CX Sales and B2B Service](#)

### Import Access Groups and Group Members

You can import access groups and group members into your sales environment rather than performing these tasks manually in the UI. To import access groups and group members, create two import files, one for each of the following objects:

- **Access Groups**
• Access Group Members

Import the access groups first, then the group members.

**Note:** You can't import system groups or add members to system groups using the import functionality. If you export a system access group and then import the group data, the group is created as a custom group.

**Import Access Groups**

1. Create a CSV file containing the list of the access groups you want to import.
   Create columns to specify these values for each group you import:
   - A name for the group (Name)
   - A number for the group (AccessGroupNumber)
   
   You can optionally enter a group description (Description) and a column to indicate if the group is active or not (ActiveFlag).
2. Navigate to the Manage Imports page (**Tools > Import Management**), then click **Create Import Activity**.
3. Assign a name to the import in the **Name** field.
4. In the **Object** field, select **Access Groups**.
5. In the **File Name** field, select the CSV file you created in step 1, then click **Next**.
6. On the Create Import Activity: Map Fields page, review the field mappings, then click **Next**.
7. On the Create Import Activity: Review and Submit page, click **Submit**.

**Import Access Group Members**

1. Create a CSV file containing the list of access group members you want to import.
   For each group member, create columns to specify these values:
   - PartyNumber column. This is the user’s resource registry ID. This value is available on the Add: Group Members UI in the Sales and Service Access Management work area.
   - AccessGroupNumber column. The number of the group you want to assign the user to. This number must match the number of one of the groups you previously imported.
2. Navigate to the Manage Imports page (**Tools > Import Management**), then click **Create Import Activity**.
3. Assign a name to the import in the **Name** field.
4. In the **Object** field, select **Access Group Members**.
5. In the **File Name** field, select the CSV file you created in step 1, then click **Next**.
6. On the Create Import Activity: Map Fields page, review the field mappings, then click **Next**.
7. On the Create Import Activity: Review and Submit page, click **Submit**.

Navigate to the Access Groups page and verify that you can see the access groups you imported and that they're assigned the correct members. Notice that imported users are listed in the Member Type column as **Manual** users because they weren't added to the group through group membership rule processing.

**Export Access Groups, Members, and Rules**

Using the export management framework, you can export access group objects from your sales environment into CSV files. The access group objects you can export include:

• Access groups
• Access group members

• Access group rules (group membership rules, and predefined and custom object sharing rules)

Each access group rule can have multiple rule conditions and can be assigned to multiple access groups (rule candidates) so you can also choose to export only rule conditions or only rule candidates.

| Note: | You can’t export access extension rules. |

For each object you choose to export, you can select the data attributes you want to download for data analysis. You can also use filters to specify the range of access groups, members or rules to export. For example, you can use filters to export object access group rules for specific objects, such as Account. Ensure that any custom objects or attributes are synchronized before you export your access group rules.

Here’s how to export access group object details to a CSV file.

1. Navigate to **Tools > Export Management**.
2. On the Manage Exports page, click **Create Export Activity**.
3. On the Create Export Activity: Enter Export Options page, select a name for the export job in the **Name** field.
4. From the **Object** drop-down list, select one of the access group objects:
   - Access Groups
   - Access Group Members
   - Access Group Rule
   - Access Group Rule Candidate
   - Access Group Rule Condition

Access Group Rule Candidate and Access Group Rule Condition are child objects of Access Group Rule so you can export all three objects at the same time by selecting the Access Group Rule object. You can also export each object individually.

The **File Name** field is automatically filled with a file name to reflect the object type you selected. For example, if you selected Access Group Rule as the object to export, a file name similar to AccessGroupRule20200731_1307.zip is generated for you. If you select Access Group Rule Candidate, then a file name such as AccessGroupRuleCandidate20200731_1310.zip is automatically entered.

5. In the Advanced Options region, select **Language Independent Header** to ensure that column headers display correctly in the exported CSV file, then click **Next**.

6. On the Create Export Activity: Map Fields page, you can select the fields to export.

   Alternatively, you can select an existing mapping from the **Export Mapping** drop-down list which shows the maps that were used in earlier export jobs.

7. In the Export Objects area, select the child objects, if any, that you want to export by selecting the **Enabled** check box.

8. In the Attributes area, select the attributes you want to export for the selected object or objects by double-clicking the attribute in the **Available Fields** list or manually moving the attribute from the **Available Fields** list to the **Selected Fields** list.

   For example, for the Access Group object, you might select these fields: Number, Name, Description, Active.

9. You must provide a filter criterion for at least the top-level object. To filter the records to export using conditions, in the Export Objects area, click the **Filter Name** icon to display the **Filter Name** dialog box.
10. To create the filter:
   a. On the Fields tab select the attribute you want to use to filter the access group data that’s exported and click the Insert button.
   b. In the Script Edit window, provide the filter conditions for the selected attribute using the available operators such as AND, OR, =, and !=.
   c. After creating the filter criteria script, click Validate Script.

Here are some examples of filter criteria you might define for different access group objects.

<table>
<thead>
<tr>
<th>Access Group Export Object</th>
<th>Filter Condition</th>
<th>Filter Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Group Rule</td>
<td>Export all access group rules including object sharing rules and group membership rules.</td>
<td>ObjectName != 'Null'</td>
</tr>
<tr>
<td>Access Group Rule</td>
<td>Export group membership rules only.</td>
<td>ObjectName = 'Resources'</td>
</tr>
<tr>
<td>Access Group Rule</td>
<td>Export object sharing rules only.</td>
<td>ObjectName != 'Resources'</td>
</tr>
<tr>
<td>Access Group Rule</td>
<td>Export access group rules for the Account object.</td>
<td>ObjectName = 'Account'</td>
</tr>
<tr>
<td>Access Groups</td>
<td>Export data for a specific access group.</td>
<td>GroupName='France_Admin_Group'</td>
</tr>
<tr>
<td>Access Groups and Access Group Members</td>
<td>Export all access groups with a specific member.</td>
<td>EmailAddress='email_address'</td>
</tr>
</tbody>
</table>

11. If the script validates successfully, click Save and Close to save the filter, then click Next.
12. On the Create Export Activity: Review and Submit page, review the export activity configuration, then click Submit to activate the export activity.
13. On the Manage Exports page, review the export job and when it completes, click the ZIP file link in the Exported Data File column to download the exported file. Verify that the file contains all the information you wanted to export.

Related Topics
- How You Monitor Export Activity

Migrate Access Group Rules Setup Data

You can migrate object sharing rules setup data from one environment to another using the setup import and export functionality available in the Setup and Maintenance work area. If you export and import rules setup data using this option, make sure that any access groups and group members that exist in the source environment are created in the target environment before you import the object sharing rules. Otherwise, the rules aren’t assigned correctly.

Perform the migration steps in this sequence:

1. (Optional) Perform a configuration set migration to move any configurations you have made in the source environment, such as creating custom objects or attributes, to the target environment.
For information on this step, see the guide Configuring and Extending Applications.

2. Synchronize all custom objects and attributes you migrated in the previous step using the Manage Object Sharing Assignment Objects task in the Setup and Maintenance work area:
   a. Sign in as a setup user and navigate to the Setup and Maintenance work area.
   b. Select the Sales offering, then search for and select the Manage Object Sharing Assignment Objects task.
   c. From the Actions menu, select Export to CSV File.
   d. Once the rules are exported, download and extract the CSV file.
   e. In the target environment, import the CSV file you just extracted by selecting the Manage Object Sharing Assignment Objects task in the Setup and Maintenance work area.
   f. From the Actions menu, select Import from CSV File.

   You don’t have to run the Synchronize Custom Objects and Fields option on the Object Sharing Rules page in the target environment after the import process completes.

3. Export and then import access groups and group members from your source environment to your target environment using the standard export and import framework. See the import and export topics in this chapter for information on these tasks.

4. Export and import object sharing rules:
   a. In your source environment, export object sharing rules by navigating to the Setup and Maintenance work area, then selecting the Sales offering.
   b. Search for and select the Manage Object Sharing Rules task.
   c. From the Actions menu, select Export to CSV File.
   d. Once the rules are exported, download and extract the CSV file.
   e. In your target environment, import the CSV file containing the object sharing rules you just exported by selecting the Manage Object Sharing Rules task in the Setup and Maintenance work area.
   f. From the Actions menu, select Import from CSV File.
   g. Once the rules are imported, verify that the object sharing rules and group membership rules are displaying correctly in your environment.

For detailed information on importing and exporting setup data, see the topic Export and Import CSV File Packages. For an example of importing and exporting assignment manager objects, see the topic Example of Uploading Assignment Objects and Rules Setup Data to a CSV File.

**Related Topics**

- Example of Uploading Assignment Objects and Rules Setup Data to a CSV File
- Export and Import CSV File Packages

### How Data Security Policies Map to Access Group Predefined Rules

You can now use the predefined object sharing rules available with access groups to give users the same access to object data that the predefined data security policies provide. The tables in this topic show, for supported objects, the predefined rule that corresponds to each of the existing data security policies.
Account Object Mapping

This table shows how the predefined data security policies for the Account object map to predefined access group rules.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZBS1</td>
<td>Access the sales party for table HZ_PARTIES where they are the account owner</td>
<td>Account</td>
<td>AccountOwner</td>
<td>AccountPR1</td>
<td>Accounts where the access group member is the account owner</td>
<td>ACCOUNTOWNER</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZBS1</td>
<td>Access the sales party for table HZ_PARTIES where they are in the management chain of the account owner</td>
<td>Account</td>
<td>AccountOwnerHierarchy</td>
<td>AccountPR2</td>
<td>Accounts where the access group member is in the management chain of the account owner</td>
<td>ACCOUNTOWNERHIER</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where user is in the sales account team</td>
<td>Account</td>
<td>AccountTeam</td>
<td>AccountPR3</td>
<td>Accounts where the access group member is on the account team</td>
<td>ACCOUNTTEAM</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where user is in the sales account team with edit access</td>
<td>Account</td>
<td>AccountTeamWithEditAccess</td>
<td>AccountPR5</td>
<td>Accounts where the access group member is on the account team with edit access</td>
<td>ACCOUNTTEAMWITHEDIT</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where</td>
<td>Account</td>
<td>AccountTeamWithFullAccess</td>
<td>AccountPR7</td>
<td>Accounts where the access group member</td>
<td>ACCOUNTTEAMWITHFULL</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account</td>
<td>AccountPR4</td>
<td>Accounts</td>
<td>ACCOUNTTEAMHIER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where the access group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member is in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>management chain of a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resource who is on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>account team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>is on the account team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>with full access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account</td>
<td>AccountPR6</td>
<td>Accounts</td>
<td>ACCOUNTTEAMHIERWITH</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where the access group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member is in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>management chain of a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resource who is on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>account team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>with edit access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account</td>
<td>AccountPR8</td>
<td>Accounts</td>
<td>ACCOUNTTEAMHIERWITH</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where the access group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member is in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>management chain of a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resource who is on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>account team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>with full access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account</td>
<td>AccountPR9</td>
<td>Accounts</td>
<td>ACCOUNTTERRITORY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where the access group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member is in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>territory team</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account Territory Team Hierarchy</td>
<td>AccountPR10</td>
<td>member is a member of the territory associated with the account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account Territory Owner</td>
<td>AccountPR11</td>
<td>Accounts where the access group member is the owner of the territory associated with the account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Account</td>
<td>Account Territory Owner Hierarchy</td>
<td>AccountPR12</td>
<td>Accounts where the access group member is the owner of the territory that is an ancestor of the territory associated with the account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES for all sales parties in the enterprise</td>
<td>Account</td>
<td>All Parties</td>
<td>AccountPR13</td>
<td>Access all parties</td>
<td>GLOBAL_ACCOUNT</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESHZ5</td>
<td>Access the trading community party for table HZ_PARTIES all accounts in the enterprise</td>
<td>Account</td>
<td>All Accounts</td>
<td>AccountPR14</td>
<td>Access all accounts</td>
<td>ALLACCOUNTS</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES for all prospects in the enterprise</td>
<td>Account</td>
<td>All Prospects</td>
<td>AccountPR15</td>
<td>Access all prospects</td>
<td>ALLPROSPECTS</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES for all customers in the enterprise</td>
<td>Account</td>
<td>All Customers</td>
<td>AccountPR16</td>
<td>Access all customers</td>
<td>ALLCUSTOMERS</td>
</tr>
</tbody>
</table>

**Contact Object Mapping**

This table shows how the predefined data security policies for the Contact object map to predefined access group rules.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZBS1</td>
<td>Access the sales party for table HZ_PARTIES where they are the account owner</td>
<td>Contact</td>
<td>Contact Owner</td>
<td>ContactPR1</td>
<td>Contacts where the access group member is the contact owner</td>
<td>CONTACTOWNER</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZBS1</td>
<td>Access the sales party for table HZ_PARTIES where they are in the management chain of the account owner</td>
<td>Contact</td>
<td>Contact Owner Hierarchy</td>
<td>ContactPR2</td>
<td>Contacts where the access group member is in the management chain of the contact owner</td>
<td>CONTACTOWNERHIER</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where user is in the sales account team</td>
<td>Contact</td>
<td>Contact Team</td>
<td>ContactPR3</td>
<td>Contacts where the access group member is on the contact team</td>
<td>CONTACTTEAM</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where user is in the sales account team with edit access</td>
<td>Contact</td>
<td>Contact Team with Edit Access</td>
<td>ContactPR5</td>
<td>Contacts where the access group member is on the contact team with edit access</td>
<td>CONTACTTEAMWITHEDIT</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES where user is in the sales account team with full access</td>
<td>Contact</td>
<td>Contact Team with Full Access</td>
<td>ContactPR7</td>
<td>Contacts where the access group member is on the contact team with full access</td>
<td>CONTACTTEAMWITHFULL</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>Contact Team Hierarchy</td>
<td>ContactPR4</td>
<td>Contacts where the access group member is in the management chain of a resource who is on the contact team</td>
<td>CONTACTTEAMHIER</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>Contact Team Hierarchy with Edit Access</td>
<td>ContactPR6</td>
<td>Contacts where the access group member is in the management chain of a resource who is on the contact team with edit access</td>
<td>CONTACTTEAMHIERWITHEDIT</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>Contact Team Hierarchy with Full Access</td>
<td>ContactPR8</td>
<td>Contacts where the access group member is on the contact team with full access</td>
<td>CONTACTTEAMHIERWITHFULL</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>Contact Territory Team</td>
<td>ContactPR9</td>
<td>Contacts where the access group member is a member of the territory associated with the contact</td>
<td>CONTACTTERRITORY</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>with the sales contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CONTACTTERRITORYHIER</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>ContactPR10</td>
<td>CONTACTTERRITORYOWNER</td>
<td>CONTACTTERRITORYOWNHIER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access the sales party for table</td>
<td></td>
<td>Contact</td>
<td>ContactPR11</td>
<td>CONTACTTERRITORYOWNER</td>
<td>CONTACTTERRITORYOWNHIER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HZ_PARTIES where user is a member of</td>
<td></td>
<td>Contact</td>
<td>ContactPR12</td>
<td>CONTACTTERRITORYOWNER</td>
<td>CONTACTTERRITORYOWNHIER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the territory that is an ancestor</td>
<td></td>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td>ALLSTANDALONECONTACTS</td>
<td></td>
</tr>
<tr>
<td>of the territory associated with</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the sales account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with the sales contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>ContactPR13</td>
<td>Access all standalone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access the sales party for table</td>
<td></td>
<td>Contact</td>
<td></td>
<td>contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HZ_PARTIES where user is the owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of the territory that is an ancestor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of the territory associated with</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Contact</td>
<td>ContactPR13</td>
<td>Access all standalone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access the sales party for table</td>
<td></td>
<td>Contact</td>
<td></td>
<td>contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HZ_PARTIES for all standalone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESHZ5</td>
<td>Contact</td>
<td>All Contacts</td>
<td>ContactPR14</td>
<td>Access all contacts</td>
<td>ALLCONTACTS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESHZ41</td>
<td>Contact</td>
<td>Internal Contacts</td>
<td>ContactPR15</td>
<td>Access internal contacts</td>
<td>INTERNALCONTACTS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESHZ19</td>
<td>Contact</td>
<td>Person Social Security Number</td>
<td>ContactPR16</td>
<td>Access person social security number</td>
<td>SOCIAL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZCITIZENSHIP</td>
<td>Contact</td>
<td>Person Citizenship Number</td>
<td>ContactPR17</td>
<td>Access person citizenship number</td>
<td>CITIZENSHIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTYSITES2</td>
<td>Access the trading community person address for table HZ_PARTY_SITE for personal addresses</td>
<td>Contact</td>
<td>Person Address</td>
<td>ContactPR18</td>
<td>Access person address</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZCONTACTPOI</td>
<td>Access the trading community person phone for table HZ_CONTACT_F for personal phone numbers</td>
<td>Contact</td>
<td>Person Mobile Phone Number</td>
<td>ContactPR19</td>
<td>Access person mobile phone number</td>
<td>MOBILE</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZCONTACTPOI</td>
<td>Access the trading community person e-mail for table HZ_CONTACT_F for personal e-mail</td>
<td>Contact</td>
<td>Person Home Phone and Personal Email</td>
<td>ContactPR20</td>
<td>Access person home phone and personal email</td>
<td>EMAILPHONE</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZADDTNLPAR1</td>
<td>Access the trading community person additional identifier for table HZ_ADDTNL_PA for all identifiers in the enterprise</td>
<td>Contact</td>
<td>Person Additional Identifier</td>
<td>ContactPR21</td>
<td>Access person additional identifier</td>
<td>ADDITIONAL</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES for all prospects in the enterprise</td>
<td>Contact</td>
<td>All Prospects</td>
<td>ContactPR22</td>
<td>Access all prospects</td>
<td>ALLCONTACTSPROSPECTS</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Trading Community Party</td>
<td>HZPARTIESZCM</td>
<td>Access the sales party for table HZ_PARTIES for all customers in the enterprise</td>
<td>Contact</td>
<td>All Customers</td>
<td>ContactPR23</td>
<td>Access all customers</td>
<td>ALLCONTACTSCUSTOMERS</td>
</tr>
</tbody>
</table>

### Lead Object Mapping

This table shows how the predefined data security policies for the Lead object map to predefined access group rules.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a resource in the lead sales team</td>
<td>Lead</td>
<td>Lead Team</td>
<td>LeadPR4</td>
<td>Leads where the access group member is on the lead team</td>
<td>LEADTEAM</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a resource in the territory assigned to the sales lead</td>
<td>Lead</td>
<td>Lead Territory Team</td>
<td>LeadPR8</td>
<td>Leads where the access group member is a member of a territory associated with the lead</td>
<td>LEADTERR</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are an administrator of the</td>
<td>Lead</td>
<td>Lead Owner Organization Administrator</td>
<td>LeadPR2</td>
<td>Leads where the access group member is the administrator of the resource</td>
<td>LEADOOWNERORGADMIN</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are the owner of the sales lead</td>
<td>Lead</td>
<td>Lead Owner</td>
<td>LeadPR1</td>
<td>Leads where the access group member is the lead owner</td>
<td>LEADOWNER</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a resource in the lead sales team with full access</td>
<td>Lead</td>
<td>Lead Team With Full Access</td>
<td>LeadPR5</td>
<td>Leads where the access group member is on the lead team with full access</td>
<td>LEADTEAMWITHFULL</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS for all sales leads in the enterprise</td>
<td>Lead</td>
<td>All Leads</td>
<td>LeadPR12</td>
<td>Access all leads</td>
<td>GLOBAL_LEAD</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS for all retired, qualified, unqualified leads in the enterprise</td>
<td>Lead</td>
<td>All Leads</td>
<td>LeadPR12</td>
<td>Access all leads</td>
<td>GLOBAL_LEAD</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a member of a territory</td>
<td>Lead</td>
<td>Lead Territory Team</td>
<td>LeadPR8</td>
<td>Leads where the access group member is a member of a territory</td>
<td>LEADTERRITORY</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>-------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKL_LM_LEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the sales lead territory team or a territory resource with a descendant territory in the sales lead territory team</td>
<td>Lead</td>
<td>Lead Territory Team Hierarchy</td>
<td>LeadPR9</td>
<td>Leads where the access group member is a member of a territory that is an ancestor of a territory associated with the lead</td>
<td>LEADTERRITORYHIER</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKL_LM_LEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS for all retired leads in the enterprise</td>
<td>Lead</td>
<td>All Nonconverted Leads</td>
<td>LeadPR10</td>
<td>Access all nonconverted leads</td>
<td>ALLNONCONVERTEDLEADS</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKL_LM_LEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS for all partner leads in the enterprise</td>
<td>Lead</td>
<td>All Partner Leads</td>
<td>LeadPR11</td>
<td>Access all partner leads</td>
<td>ALLPARTNERLEADS</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKL_LM_LEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS</td>
<td>Lead</td>
<td>Lead Team Hierarchy</td>
<td>LeadPR7</td>
<td>Leads where the access group</td>
<td>LEADTEAMHIERWITHFUL</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>MKL_LM_LEADS</td>
<td>MKLLMLEADSM</td>
<td>Lead</td>
<td>with Full Access</td>
<td></td>
<td>member is in the management chain of a resource who is on the lead team with full access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a manager in the management hierarchy of a resource in the lead sales team with full access</td>
<td>Lead Owner Hierarchy</td>
<td>LeadPR3</td>
<td>Leads where the access group member is in the management chain of the lead owner</td>
<td>LEADOWNERHIER</td>
<td></td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a manager in the management hierarchy of a resource in the lead sales team</td>
<td>Lead Team Hierarchy</td>
<td>LeadPR6</td>
<td>Leads where the access group member is in the management chain of a resource who is on the lead team</td>
<td>LEADTEAMHIER</td>
<td></td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are in the management hierarchy of the owner of the lead</td>
<td>Lead Team Hierarchy</td>
<td>LeadPR6</td>
<td>Leads where the access group member is in the management chain of a resource who is on the lead team</td>
<td>LEADTEAMHIER</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a member of the lead sales account team or in the management chain of an lead sales account team member</td>
<td>Lead</td>
<td>Account Team</td>
<td>AccountPR3</td>
<td>Accounts where the access group member is on the account team</td>
<td>ACCOUNTTEAM</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a member of the lead sales account team or in the management chain of an lead sales account team member</td>
<td>Lead</td>
<td>Account Team Hierarchy</td>
<td>AccountPR4</td>
<td>Accounts where the access group member is in the management chain of a resource who is on the account team</td>
<td>ACCOUNTTEAMHIER</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the lead sales account territory team or a territory resource with a descendant</td>
<td>Lead</td>
<td>Account Territory</td>
<td>AccountPR9</td>
<td>Accounts where the access group member is a member of the territory associated with the account</td>
<td>ACCOUNTTERRITORY</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Sales Lead MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the lead sales account territory team or a territory resource with a descendant territory in the lead sales account territory team</td>
<td>Lead</td>
<td>Account</td>
<td>AccountPR10</td>
<td>Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account</td>
<td>ACCOUNTTERRITORYHIER</td>
<td></td>
</tr>
<tr>
<td>Sales Lead MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the lead sales account territory team or a territory resource with a descendant territory in the lead sales account territory team</td>
<td>Lead</td>
<td>Business Unit Leads</td>
<td>LeadPR13</td>
<td>Leads in the business units that the access group member is associated with</td>
<td>BULEADS</td>
<td></td>
</tr>
<tr>
<td>Sales Lead MKLMLMLEADSM</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales account team,</td>
<td>Lead</td>
<td>Account Team</td>
<td>AccountPR3</td>
<td>Accounts where the access group member is on the account team</td>
<td>ACCOUNTTEAM</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSM</td>
<td>Lead</td>
<td>Account Team</td>
<td>AccountPR4</td>
<td>Accounts where the access group member is in the management chain of a resource who is on the account team</td>
<td>ACCOUNTTEAMHIER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Territory</td>
<td>AccountPR9</td>
<td>Accounts where the access group member is a member of the territory associated with the account</td>
<td>ACCOUNTTERRITORY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Team Hierarchy</td>
<td>AccountPR10</td>
<td>Accounts where the access group member is a member of the territory that is an ancestor of the territory</td>
<td>ACCOUNTTERRITORYHIER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>潇潇</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSZB</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory team or upward territory hierarchy</td>
<td>Lead</td>
<td>Lead Team</td>
<td>LeadPR4</td>
<td>Leads where the access group member is on the lead team</td>
<td>LEADTEAM</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSZB</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory team or upward territory hierarchy</td>
<td>Lead</td>
<td>Lead Team Hierarchy</td>
<td>LeadPR6</td>
<td>Leads where the access group member is in the management chain of a resource who is on the lead team</td>
<td>LEADTEAMHIER</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSZB</td>
<td>Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory</td>
<td>Lead</td>
<td>Lead Territory Team</td>
<td>LeadPR8</td>
<td>Leads where the access group member is a member of a territory associated with the lead</td>
<td>LEADTERRITORY</td>
</tr>
</tbody>
</table>
### Access Groups

#### Predefined Rule Name

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Lead</td>
<td>MKLLMLEADSZB</td>
<td>Lead</td>
<td>LeadPR9</td>
<td></td>
<td>Leads where the access group member is a member of a territory that is an ancestor of a territory associated with the lead</td>
<td>LEADTERRITORYHIER</td>
</tr>
</tbody>
</table>

Advanced permissions are defined for some of the Lead data security policies. Advanced permissions let you refine the access provided by a data security policy. This table shows how the advanced permissions available with Lead data security policies map to predefined access group rules.

<table>
<thead>
<tr>
<th>Data Security Policy Business Object</th>
<th>Data Security Policy Advanced Permission Name</th>
<th>Access Group Object</th>
<th>Predefined Rule Name</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Lead</td>
<td>View Sales Lead</td>
<td>Lead</td>
<td>Any predefined rule</td>
<td>Read, Update, Delete, Full</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>Update Sales Lead</td>
<td>Lead</td>
<td>Any predefined rule</td>
<td>Update, Full</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>Delete Sales Lead</td>
<td>Lead</td>
<td>Any predefined rule</td>
<td>Delete, Full</td>
</tr>
<tr>
<td>Sales Lead</td>
<td>Convert Sales Lead</td>
<td>Lead</td>
<td>Any predefined rule</td>
<td>Full</td>
</tr>
</tbody>
</table>

### Opportunity Object Mapping

This table shows how the predefined data security policies for the Opportunity object map to predefined access group rules.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity</td>
<td>MOOOPTYMOC</td>
<td>Access the opportunity for table MOO_OPTY where they selected records where I am on the team on the sales UI</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR3</td>
<td>Opportunities</td>
<td>OPTYTEAM</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYMOC</td>
<td>Access the opportunity for table MOO_OPTY where they selected records I own on the sales UI</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR1</td>
<td>Opportunities</td>
<td>OPTYOWNER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYMOC</td>
<td>Access the opportunity for table MOO_OPTY where they selected records my subordinates own on the sales UI</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR2</td>
<td>Opportunities</td>
<td>OPTYOWNERHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYMOC</td>
<td>Access the opportunity for table MOO_OPTY where they selected records my subordinates are on the team on the sales UI</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR6</td>
<td>Opportunities</td>
<td>OPTYTEAMHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYMOC</td>
<td>Access the opportunity for table MOO_OPTY where they selected Opportunity Team hierarchy</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR9</td>
<td>Opportunities</td>
<td>OPTYTERRITORYOWNER</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>records in my territory on the sales UI</td>
<td>MOOOPTYMOO</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR1</td>
<td>Opportunities where the access group member is the owner of a territory that is an ancestor of a territory associated with the opportunity</td>
<td>OPTYTERRITORYOWNERHIER</td>
<td></td>
</tr>
<tr>
<td>Access the opportunity for table MOO_OPTY where they selected records in my territory hierarchy on the sales UI</td>
<td>MOOOPTYMOO</td>
<td>Opportunity</td>
<td>All Opportunities</td>
<td>OpportunityPR1</td>
<td>Access all opportunities</td>
<td>GLOBAL_OPPORTUNITY</td>
<td></td>
</tr>
<tr>
<td>Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity sales account territory team</td>
<td>MOO_OPTYACC</td>
<td>Opportunity</td>
<td>Account Territory</td>
<td>AccountPR3</td>
<td>Accounts where the access group member is on the account team</td>
<td>ACCOUNTTEAM</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTYACC</td>
<td>Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity sales account territory team</td>
<td>Opportunity</td>
<td>Account Territory Hierarchy</td>
<td>AccountPR4</td>
<td>Accounts where the access group member is in the management chain of a resource who is on the account team</td>
<td>ACCOUNTTEAMHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_ADMIN</td>
<td>Access the opportunity for table MOO_OPTY for all opportunities in the business units that they are authorized within</td>
<td>Opportunity</td>
<td>Business Unit Opportunities</td>
<td>OpportunityPR15</td>
<td>Opportunities in the business units that the access group member is associated with</td>
<td>BUOPPORTUNITIES</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_EDIT</td>
<td>Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales team member with edit or full access</td>
<td>Opportunity</td>
<td>Opportunity Team Hierarchy with Edit or Full Access</td>
<td>OpportunityPR7</td>
<td>Accounts where the access group member is in the management chain of a resource who is on the opportunity team with edit or full access</td>
<td>OPTYTEAMHIERWITHEDIT</td>
</tr>
<tr>
<td>Data Security Policy Predefined Instance Set</td>
<td>Data Security Policy Predefined Condition Name</td>
<td>Access Group Object</td>
<td>Predefined Rule Name</td>
<td>Predefined Rule Number</td>
<td>Predefined Condition Name</td>
<td>Predefined Condition Code</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_EDIT</td>
<td>Opportunity</td>
<td>Opportunity Team with Edit Or Full Access</td>
<td>OpportunityPR4</td>
<td>Opportunities where the access group member is on the opportunity team with edit or full access</td>
<td>OPTYTEAMWITHEDITORPR4</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_FOREI</td>
<td>Opportunity</td>
<td>Opportunity Partner</td>
<td>OpportunityPR4</td>
<td>Opportunities associated with a partner organization</td>
<td>OPTYANYPARTNERORG</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_FOREI</td>
<td>Opportunity</td>
<td>Partner Team</td>
<td>PartnerPR4</td>
<td>Partners where the access group member is a resource on the partner team</td>
<td>PARTNERTEAM</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_FOREI</td>
<td>Opportunity</td>
<td>Opportunity Partner Company</td>
<td>OpportunityPR4</td>
<td>Opportunities where the access group member is a member of the partner company associated with the opportunity</td>
<td>OPTYPARTNERCOMP</td>
<td></td>
</tr>
</tbody>
</table>
## Access Groups

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPRT</td>
<td>Opportunities where the access group member is a member of the child partner company associated with the opportunity</td>
<td>OPTYPARTNERHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_FULL</td>
<td>Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales team member with full access</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR8</td>
<td>Opportunities where the access group member is in the management chain of a resource who is on the opportunity team with full access</td>
<td>OPTYTEAMHIERWITHFULL</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_FULL</td>
<td>Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with full access</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR5</td>
<td>Opportunities where the access group member is on the opportunity team with full access</td>
<td>OPTYTEAMWITHFULL</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_TERR</td>
<td>Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity territory team or a territory resource</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPRT</td>
<td>Opportunities where the access group member is a member of a territory associated with the opportunity</td>
<td>OPTYTERRITORY</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_TERR_HIER</td>
<td>Opportunity</td>
<td>Opportunity Territory Team Hierarchy</td>
<td>OpportunityPR1</td>
<td>Opportunities where the access group member is a member of a territory that is an ancestor of a territory associated with the opportunity</td>
<td>OPTYTERRITORYHIER</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_VIE</td>
<td>Opportunity</td>
<td>Account Team</td>
<td>AccountPR3</td>
<td>Accounts where the access group member is on the account team</td>
<td>ACCOUNTTEAM</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_VIE</td>
<td>Opportunity</td>
<td>Opportunity Owner Hierarchy</td>
<td>OpportunityPR2</td>
<td>Opportunities where the access group member is in the management chain of the opportunity owner</td>
<td>OPTYOWNERHIER</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTY_VIE</td>
<td>Opportunity</td>
<td>OpportunityTeam</td>
<td>OpportunityPR3</td>
<td>Opportunities where the access group member is on the opportunity team</td>
<td>OPTYTEAM</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with view, edit, or full access</td>
<td>Opportunity</td>
<td>OpportunityTeam</td>
<td>Opportunities where the access group member is on the opportunity team</td>
<td>OPTYTEAM</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>OpportunityTeam</td>
<td>Opportunities where the access group member is on the opportunity team</td>
<td>OPTYTEAMHIER</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOO_OPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or</td>
<td>Opportunity</td>
<td>OpportunityTeam</td>
<td>Opportunities where the access group member is in the management chain of a resource who is on the opportunity team</td>
<td>OPTYTEAMHIER</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPSYZBS9</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR1</td>
<td>OpportunityTerritory</td>
<td>OPTYTERRITORY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy</td>
<td>OpportunityTerritory Team</td>
<td></td>
<td>Opportunities where the access group member is a member of a territory associated with the opportunity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPSYZBS9</td>
<td>Opportunity</td>
<td>Opportunity</td>
<td>OpportunityPR1</td>
<td>OpportunityTerritoryTeamH</td>
<td>OPTYTERRITORYHIER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy</td>
<td>OpportunityTerritoryTeamH</td>
<td></td>
<td>Opportunities where the access group member is a member of a territory that is an ancestor of a territory associated with the opportunity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPSYZBS9</td>
<td>Opportunity</td>
<td>Account</td>
<td>AccountPR3</td>
<td>Accounts</td>
<td>ACCOUNTTEAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of</td>
<td>Account Team</td>
<td></td>
<td>Accounts where the access group member is on the account team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>opportunity account team, account territory team or upward territory hierarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Account Team Hierarchy</td>
<td></td>
<td></td>
<td>ACCOUNTTEAMHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Account Territory</td>
<td>AccountPR9</td>
<td>Accounts where the access group member is a member of the territory associated with the account</td>
<td>ACCOUNTTERRITORY</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Account Territory Hierarchy</td>
<td>AccountPR10</td>
<td>Accounts where the access group member is a member of the territory</td>
<td>ACCOUNTTERRITORYHIER</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Contact Team</td>
<td></td>
<td>that is an ancestor of the territory associated with the account</td>
<td>CONTACTTEAM</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Contact Team Hierarchy</td>
<td>ContactPR4</td>
<td>Contacts where the access group member is on the contact team</td>
<td>CONTACTTEAMHIER</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Contact Team</td>
<td></td>
<td>that is an ancestor of the territory associated with the account</td>
<td>CONTACTTEAM</td>
</tr>
<tr>
<td>Opportunity</td>
<td>MOOOPTYZBS9</td>
<td>Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy</td>
<td>Opportunity</td>
<td>Contact Territory</td>
<td>ContactPR9</td>
<td>Contacts where the access group member is a</td>
<td>CONTACTTERRITORY</td>
</tr>
</tbody>
</table>
Advanced permissions are defined for some of the Opportunity data security policies. Advanced permissions let you refine the access provided by a data security policy. This table shows how the advanced permissions available with Opportunity data security policies map to predefined access group rules.

<table>
<thead>
<tr>
<th>Data Security Policy Business Object</th>
<th>Data Security Policy Advanced Permission Name</th>
<th>Access Group Object</th>
<th>Predefined Rule Name</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity</td>
<td>Manage Opportunity General Profile</td>
<td>Opportunity</td>
<td>Any predefined rule</td>
<td>Update, Full</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Manage Opportunity Restricted Profile</td>
<td>Opportunity</td>
<td>Any predefined rule</td>
<td>Delete, Full</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Manage Opportunity Revenue</td>
<td>Opportunity</td>
<td>Any predefined rule</td>
<td>Full</td>
</tr>
<tr>
<td>Data Security Policy Business Object</td>
<td>Data Security Policy Advanced Permission Name</td>
<td>Access Group Object</td>
<td>Predefined Rule Name</td>
<td>Access Level</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Manage Opportunity Team</td>
<td>Opportunity</td>
<td>Any predefined rule</td>
<td>Full</td>
</tr>
<tr>
<td>Opportunity</td>
<td>View Opportunity</td>
<td>Opportunity</td>
<td>Any predefined rule</td>
<td>Read, Update, Delete, Full</td>
</tr>
</tbody>
</table>
Security for Sales 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 subject areas 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 CX Security Reference for CX Sales and B2B Service
Describes the sales application security reference implementation and includes descriptions of all the predefined data that is included in the security reference implementation for an offering.

- **Oracle CX Sales Creating and Administering Analytics**

  Explains how to view and work with analytics and reports.

- **Oracle CX Sales and B2B Service Subject Areas for Transactional Business Intelligence**

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

### 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>
<tr>
<td>Permission</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Traverse</td>
<td>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.</td>
</tr>
</tbody>
</table>

| 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/.

## Transaction Analysis Duty Roles

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

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

- Partner Channel Transaction Analysis Duty
- Partner Channel Administrative Transaction Analysis Duty
- Sales Administrative Transaction Analysis Duty
- Sales Executive Transaction Analysis Duty
- Sales Managerial Transaction Analysis Duty
- Sales Transaction Analysis Duty
- Incentive Compensation Transaction Analysis Duty
This table lists analytics and reports available to sales users. It also shows the predefined job roles that can access the different analytics and reports, and the OTBI Transactional Analysis Duty roles that provide the access.

<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.

For additional information about the job roles that secure access to sales and service subject areas, and the OTBI Transactional Analysis Duty roles assigned to each job role, see Oracle CX Sales and B2B Service Subject Areas for Transactional Business Intelligence.
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.

These are the Business Intelligence roles.

<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 isn’t assigned the BI Author role.

**BI Administrator Role**

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

**BI Publisher Data Model Developer Role**

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Users with either of these predefined job roles can manage BI Publisher data models.
For additional information about the Business Intelligence roles, see Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition.

Configure Security for Oracle Transactional Business Intelligence

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

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles, for example, Sales Managerial Transaction Analysis Duty. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.

- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to 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. You also can't copy any role with a role code prefix of OBIA, for example, Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS_GENERIC_DUTY). But you can configure reporting security according to your security requirements as described here.

Modifying Transaction Analysis Duty Role Assignments

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

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

Modifying Business Intelligence Role Assignments

The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle 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. You can also add the BI Administrator Role to custom job roles if you have users who need to be able to perform high-level tasks in Business Intelligence, such as work with catalog groups.

Related Topics

- BI Administrator Permissions
View Reporting Roles

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

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

View the Reporting Roles Assigned to a Job Role

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

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

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

View the Reporting Roles You Are Assigned

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

1. Select Navigator > Tools > Reports and Analytics to open the Reports and Analytics work area.
2. Click the Browse Catalog 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.
Display Direct Report Data in Participant Manager Reports

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

In the Setup and Maintenance work area:

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

Add the Security Profile

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

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

Refresh the Manager Hierarchy

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

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

Can I configure Oracle Transactional Business Intelligence duty roles?

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

Overview

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

For additional information about managing PII data, or about configuring access to PII data, see the guide Implementing Customer Data Management for CX Sales and B2B Service at http://docs.oracle.com.

How to Protect Personally Identifiable Information

The data or information that's used to uniquely identify a contact, or locate a person is called personally identifiable information (PII), 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 must assign the required PII data policies to the custom job role in the Security Console. The IT Security Manager can also add data policies for other PII data to seeded job roles.

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

<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>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>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>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_SITE_USES 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_SITE_USES 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>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>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>
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 can’t 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's 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 having common control over one or more legal entities.

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's 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

resource role
The role the user plays in the sales organization. The resource role appears as the person’s title in the Resource Directory.

role
Controls access to application functions and data.

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 area
A set of pages containing the tasks, searches, and other content you need to accomplish a business goal.

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.